An action research derived piezoelectric approach for information risk management

Meng Chow Kang

Southern Cross University

Publication details
Copyright MC Kang 2008
An Action Research Derived Piezoelectric Approach for Information Risk Management

Meng-Chow Kang
Master of Science (Information Security)
Royal Holloway and Bedford New College, University of London

Submitted in fulfillment of the requirements for the
Degree of Doctor of Philosophy

April 2008
Abstract (with keywords)

Keywords: Information Security; Risk Management; Information Protection; Security Management; Information Risk; Risk Analysis; Security Strategy; Responsiveness; Piezoelectric.

Managing information risk have been recognized as an important part of business enterprises and government organizations to address related threats and vulnerabilities, ensure compliance with regulations and best practices, demonstrate due diligence to shareholders and customers, and ensure maximum profit with minimum cost. As observed from the past 16 years of practice as an information risk practitioner, however, there has been a lack of strategic and systemic thinking and limited literature providing suitable methodology and approach for achieving the desired outcomes of managing information risk in a changing risk environment.

The purpose of this study was to identify or develop a suitable approach for managing information risk in the changing risk environment of enterprise organizations, taking into consideration the knowledge gaps in the existing literature, and issues and dilemmas observed in the practice.

The social-technical nature of the problem and the use of the workplace as a research context suggested the use of the action research methodology in the study.

Using action research, the study established that existing baseline practices have been mostly control-oriented, focusing on compliance, addressing only known and probably high risk issues that were subjectively identified and assessed. Such approaches could not gain stakeholders’ commitments to investing and taking proactive actions on risk issues if they were not identified as compliance related. Instead of being prepared and ready to respond, organizations were often surprised when new security events emerged, then reacting to recover from the incidents.

Analyzing the risk management methods and practices adopted, and the changing nature of the risk environment, the study affirmed that information risk in organizations is such that it cannot be completely identified, and accurately risk assessed and managed with existing approaches.

The existing baseline and risk management approaches should be complemented with social-technical tools and processes to gain stakeholders recognition and commitment.
to actions for information risk management. A selection of action research and systemic thinking tools and techniques were tested in the study as suitable for focusing on the social aspects of information risk management.

In addition to addressing known risks, organizations should be prepared and be responsive to emerging and new security issues and events. The study conceptualized and developed a substantive theory of information security risk management, known as the piezoelectric theory. The piezoelectric theory states that if the design of information security practices of organization systems enables a prompt re-alignment of the systems, satisfying the systemic requirements for the changing risk condition of the systems environment, the potential negative effects of the new risk condition of the systems environment will be balanced or counter-acted by the re-alignment activities. As a result of the piezoelectric behavior in organizational systems, as evidenced in this study, the consequences of the emerging or new risk condition of the environment will likely incur a reduced impact to the organization systems. Results of the study also showed that the significance of the consequences relates inversely to the security readiness, and thus, the responsiveness of the organization. Readiness relates to the organization’s preparedness to re-align its activities and take the appropriate actions to balance against the negative effects of the changing risk environment in a timely and systemic manner.

The validity of the substantive piezoelectric theory was supported by case studies of actual practices in an organization, two significant security incidents, and a focusing event during the course of the study, and tested through the development and implementation of a responsive approach to information security risk management in a participating organization and two other projects.

The study resulted in five major contributions to the knowledge and practice of information risk management. They are: (1) the development of a substantive piezoelectric theory as a new approach, providing a new meaning – responsiveness – to the objectives of information risk management, which also resolves a circularity problem in existing security principles; (2) the elaboration of the responsive strategy, including the understanding of the responsive approach through the action research study, leading to the development of a systems model for establishing the desired piezoelectric behavior to achieve responsiveness in information risk management; (3) the successful adaptation and extension of existing methods and tools as tactical
means for achieving a responsive strategy in organizations and validating the 
reliability of the piezoelectric theory; (4) an improved understanding of the issues and 
dilemmas in managing information risks in organizations; and (5) the application of 
action research as a meta-methodology and research methodology, resulting in the 
above contributions to the information risk management knowledge domain, 
demonstrating another contribution to the methodological literature.

The conclusions of the development and validation of the piezoelectric theory imply 
that changes are needed to the existing theory, policy, and practice of information risk 
management. From a theoretical perspective, (1) responsiveness should be one of the 
key objectives of information security; (2) discourse in information security should 
include the principle of responsiveness as it provides a means to resolve the 
circularity problem encountered in existing principles; (3) a responsive strategy is a 
new addition to the traditional “Protect-Detect-React”, and “Detect-React-Protect” 
strategies, addressing their weaknesses and answering to the calls for more strategic 
thinking; (4) the notion of “Responsive Learning”, a combination of both Single- and 
Double-loop learning in an organization’s information risk management system is 
important for responsiveness; and (5) the study adds to the understanding and 
knowledge on action research, implying its multiple disciplinary applicability, and 
flexibility as a meta-methodology for practicing methodological pluralism.

From the policy and practice perspectives, the outcomes imply (1) an opportunity for 
policy makers to use responsiveness as a new motivation and yardstick for improving 
information risk management in organizations; (2) a new approach for audit and 
security assurance professionals to include responsiveness in their assessment to 
determine an organization or systems readiness; (3) an opportunity for technology 
innovation for infrastructure systems alignment to the technical needs of a responsive 
strategy; (4) a possible evolution of existing risk, continuity, and recovery 
management functions to a new “readiness” group focusing on responsiveness; and 
(5) a new approach for novice and experienced information risk managers to learn and 
also manage information risks issues and dilemmas in a changing risk environment.
# Table of Contents

Abstract (with keywords)......................................................................................... ii
List of Tables ........................................................................................................... viii
List of Figures .......................................................................................................... ix
Abbreviations .......................................................................................................... xi
Statement of Original Authorship.......................................................................... xii
Acknowledgement .................................................................................................. xiii

## 1 Introduction ...................................................................................................... 1
  1.1 Background and Motivations .......................................................................... 1
  1.1.1 Business, Technology, and Risk Developments ....................................... 1
  1.1.2 Common Knowledge, Standards, and Practices ....................................... 3
  1.1.3 Profession, Organizational Role and Function ....................................... 5
  1.2 Purpose of this Study ..................................................................................... 6
  1.3 Research Questions ...................................................................................... 7
  1.4 Research Methodology .................................................................................. 8
  1.5 Delimitations of scope and key assumptions .............................................. 9
  1.6 Research Outcomes ..................................................................................... 10
  1.7 Significance of this Research ....................................................................... 13
  1.8 Organization of this Dissertation ............................................................... 14

## 2 Literature Review .......................................................................................... 16
  2.1 Introduction .................................................................................................. 16
  2.2 Information Security ..................................................................................... 17
  2.3 Principles and Approaches .......................................................................... 20
    2.3.1 Security is only as strong as the weakest link ....................................... 21
    2.3.2 Defense in depth .................................................................................. 21
    2.3.3 Use of security technology .................................................................. 22
    2.3.4 Baseline security ................................................................................ 25
    2.3.5 No Perfect Security ............................................................................ 29
    2.3.6 Information Security is Information Risk Management ....................... 30
    2.3.7 A Circular Problem ............................................................................ 45
    2.3.8 IT Security Governance ....................................................................... 46
  2.4 Information Security Risk Management Strategy .......................................... 48
    2.4.1 Protect-Detect-React (PDR) ................................................................. 49
    2.4.2 Detect-React-Protect (DRP) ................................................................. 50
    2.4.3 Need for Strategic Thinking ............................................................... 52
  2.5 Information Security Program ....................................................................... 52
    2.5.1 Organization and people ...................................................................... 53
    2.5.2 Risk assessment and management ...................................................... 54
    2.5.3 Policies ............................................................................................... 54
    2.5.4 Communication .................................................................................. 58
    2.5.5 Developments ..................................................................................... 59
    2.5.6 Operational Security .......................................................................... 59
    2.5.7 Performance Measurements ............................................................... 61
  2.6 Responding to Change ................................................................................. 66
  2.7 Current Research and Social Perspectives of Information Security ............ 68
  2.8 Conclusion .................................................................................................... 71

## 3 Research Methodology ................................................................................... 75
5.5 Implications for Policy and Practice .................................................................261
5.6 Suggestions for Further Research .................................................................265
5.7 Concluding Remarks .......................................................................................267
Notes ....................................................................................................................270
Appendices ..........................................................................................................281
  Appendix A: Survey Questionnaires .................................................................282
  Appendix B: Research Log Register .................................................................290
  Appendix C: Synthesis of information security approaches based on definition used
               .................................................................303
  Appendix D: Framework for Information Risk Management .............................305
Bibliography ..........................................................................................................311
List of Tables

Table 1: Four Windows (Flood, 1999) systemic view of information risk management situation in organization ALPHA during action research cycle 1 ............................157
Table 2: Four-windows (Flood, 1999) systemic view of the information risk management situation in organization ALPHA in action research sub-cycle 3 ........193
Table 3: Summary of information security approaches based on five key aspects of the definition of information security ..........................................................304
Table 4: Laws, Regulations, and Policies Parameters .........................................306
Table 5: Management and Organization Parameters ...........................................307
Table 6: Security Services Parameters ................................................................307
Table 7: Methods and Processes Parameters ......................................................308
Table 8: Techniques and Mechanisms Parameters ...............................................309
Table 9: Guidelines and Common Practices .........................................................310
Table 10: Technology and Solutions Parameters ...............................................310
List of Figures

Figure 1: The Circular Problem of Information Security Principles ........................................45
Figure 2: Action research as a meta-methodology ........................................................................83
Figure 3: The action research cycle alternates action and critical reflection (Dick, 2001) ..............................................................................................................................84
Figure 4: Critical reflection includes a critical review of the previous step and planning for the next step (Dick, 2001) ....................................................................................85
Figure 5: A meta-methodology perspective depicting the four main research cycles encompassing the seven sub-cycles ..................................................................................97
Figure 6: Action research spirals for thesis research ....................................................................104
Figure 7: Data-driven analysis - seek disagreement and exceptions to gain better understanding and better actions (Dick, 2000b). .................................................................114
Figure 8: Dialectic model adapted from Dick (2002f) and Tay & Lim (2004; 2007) for organization CHARLIE’s implementation of a responsive security approach .................118
Figure 9: Stakeholder analysis - attitudes of stakeholders towards IRM function ..........132
Figure 10: Stakeholder analysis - Capability of stakeholders in influencing IRM Program ..........133
Figure 11: A causal view of the audit and compliance focused risk management practice in organization ALPHA at action research sub-cycle 1 ...........................................137
Figure 12: A graphical representation of common risk analysis and management approach .................................................................................................................................148
Figure 13: Common strategy in risk management .................................................................150
Figure 14: Knowles' organizational strategy for risk mitigation (Knowles, 2005) ..................151
Figure 15: A causal view of information security system ..................................................156
Figure 16: Information risk practice with Control Self-Assessment (CSA) .....................161
Figure 17: Audit review to provide assurance of adequate systems practices and behavior .................................................................161
Figure 18: Symptomatic response to audit interventions .....................................................162
Figure 19: “Shifting the burden” structure enforced with symptomatic response ........162
Figure 20: Enforcing fundamental response by IRM Program ............................................163
Figure 21: Initial five-level action map of information security risk management system .................................................................172
Figure 22: Information risk management systems incorporating stakeholders’ participation ..................................................................................................................................173
Figure 23: Progress in stakeholders' acceptance of IRM Program ........................................180
Figure 24: Lack of synergy between IRM, BCP, and DRP systems and processes ....191
Figure 25: Displacement of electrical charge due to the deflection of the lattice in a naturally piezoelectric quartz crystal (PCB Piezotronics Inc, 2002). ..................................196
Figure 26: Mapping Piezoelectric Behavior to Responsive Approach ...............................198
Figure 27: Element of uncertainty creating an invisible plane in the risk chart ..........208
Figure 28: Sources of information for Information Risk Forecasting ..................................227
Figure 29: Mapping Risk Forecasts against Requirements for Criticality Alignment ..........229
Figure 30: An information risk management system model based on the responsive approach for information risk management ..................................................................................................................233
Figure 31: Argyris and Schon's (1991b) Concept of Single and Double Loop Learning ..................................................................................................................................236
Figure 32: A macro view of the devised responsive information security risk management systems model .................................................................237
Figure 33: Incorporating Responsive Learning into Single- and Double-loop Learning ........................................................................................238
Figure 34: Resolving the circularity problem of information security principles with the introduction of piezoelectric behavior principle ..............................................241
Figure 35: Information Risk Management Framework .......................................................305
Abbreviations

AD Application Developer
AR Action Research
BIRM Business-aligned Information Risk Manager
CEO Chief Executive Officer
CIO Chief Information Officer
CISO Chief Information Security Officer
CMM Capability Maturity Model
COO Chief Operating Officer
CSA Control Self Assessment
CSO Chief Security Officer
CTO Chief Technology Officer
FLAM Five-level Action Map
FIRM Framework for Information Risk Management
INFORISK Information Risk
INFOSEC Information Security
IRM Information Risk Management
IS Information Systems
ISM Information Security Management
ISMS Information Security Management System
ISRM Information Security Risk Management/Manager
ISO International Standards Organization
IT Information Technology
ITU International Telecommunication Union
LOB Line of Business (a business division)
LOC Location Operating Committee
OPSEC Operational Security
ORC Operational Risk Capital
ORM Operational Risk Management
PDCA Plan-Do-Check-Act – an ISO-standardized management process
PAOR Plan-Act-Observe-Reflect – an Action Research cycle
RCSA Regional Chief Security Advisor
RIRO Regional Information Security Risk Officer
ROI Return on Investment
SA Security Advisor
SE Software Engineering
SEC4 Stakeholder analysis, Entry and contracting, Convergent interviewing, and Four-windows systemic view
SQL Structured Query Language
SSM Soft Systems Methodology
TCSEC Trusted Computer Security Evaluation Criteria (also known as “Orange Book”)
Statement of Original Authorship

The work presented in this dissertation is, to the best of my knowledge and belief, original, except as acknowledged in the text. The material has not been submitted, either in whole or in part, for a degree at Southern Cross University or any other university.

Meng-Chow Kang
April 2008

Copyright © Meng-Chow Kang, April 2008
Acknowledgement

I am indebted to Professor Bob Dick, my thesis supervisor, for his encouragement, guidance, and insights that led to my completion of this thesis.

This thesis would not have been possible without the constant encouragement, guidance, and shared vision of Dr Boon-Hou Tay, which I deeply appreciate. The idea of the piezoelectric metaphor originated from Boon-Hou’s insights and deep knowledge and experience in physics and electrical engineering.

I am especially grateful to Professor Pauline Reich of Waseda University, Tokyo, and Yean-Lan Thay for their editorial assistance and also constant encouragement throughout this writing. Special thanks to also many long-time friends and colleagues in the field of information security, in particular, Pearly Cheng Ai Ling, Koon-Huat Yeo, Chin-Cheng Baey, Nelson Chow, Chuan-Wei Hoo, Koji Nakao, Professor Ted Humphrey, Philip Sy, Douglas Lee, Won-Young Cho, and Steve Riley for their sharing and feedback through the various stages of this thesis.

I am also grateful to Associate Professor Stewart Hase, Associate Professor Shankar Sankaran, Emeritus Professor Alan Davies, Dr Richard Kwok, Dr Moh-Heng Goh, Dr Stephenie Chee, and Dr Eric Goh for their guidance and encouragement, and fellow researchers at the South Cross University for their sharing during the Action Learning Sets throughout this study.

I wish to also acknowledge my former colleagues and managers, Ellen McDermott, Chris Atkinson, Peter Moore, and Robert Chu for their encouragement and the role they played in my career that made this thesis possible.

This thesis would also not be possible without the constant support, understanding, and endurance of my beloved wife, Lay-Har Tan, my parents, and the rest of my family.

Thank you all.
1 Introduction

1.1 Background and Motivations

A common objective of information risk management is to ensure adequate protection of the confidentiality, integrity, and availability of information and information systems that are critical or essential to the success of the business. As an information security practitioner in this field for more than 16 years prior to conducting this study, I have observed in my practice and also gathered from those of my contemporaries that the knowledge and practice of information risk management have been lagging other management disciplines, and inadequate for supporting the needs of the practitioners in the field. To a large extent, rather than taking strategic approaches, practitioners’ practices have been based mostly on individual’s experience, trial-and-error, and in some instances, adaptation of methods from other knowledge sources and disciplines. Most practitioners have been focusing on policy compliance and primarily addressing known risk issues, then reacting to security incidents as they occurred, even though recognizing the constantly changing nature of organization risk environment. The interest to improve my practice in the field drove the undertaking of this study to identify or develop a suitable approach for managing information risk in the changing risk environment of enterprise organizations, taking into consideration the knowledge gaps in the existing literature, and the issues and dilemmas observed in the practice. My experience in this field also shaped my thinking and analysis in the subject and in formulating the research problem and developing the outcome.

This chapter introduces the thematic issues and dilemmas in information risk management leading to the formulation and justification of the research questions in the study. It follows with a brief description of the research methodology and procedure, and the primary assumptions and delimitations in the conduct of the study. The chapter then summarizes the research outcomes and highlights the significance of those outcomes before closing with an outline of the chapters that follow.

1.1.1 Business, Technology, and Risk Developments

This research began in January 2002 along with my employment with organization ALPHA. I was a member of the information risk management (IRM) team in charge
of the function in eleven cities across the Asia Pacific region. My responsibility was to manage the information security risk of ALPHA organization in the region.

During that period, when the aftermath of the September 11, 2001 incident in the United States and subsequent war in Afghanistan (Madrick, 2002; Moniz, 2003) were negatively affecting the economy worldwide, many business organizations began a series of rapid changes to reduce cost in view of a projected zero or negative growth in revenue (Yourdan, 2002). ALPHA was not excluded from this development.

One significant change occurred in ALPHA was the stepping-up of outsourcing and offshoring of information technology (IT) and back-office operation services to reduce the total cost of IT and business operations. This change required ALPHA to increase its reliance on external providers for services and operations, and created an extended trust environment that the business units have increasingly depended upon to meet their goals. Such a change was then common in the industry (McDougall, 2002a, 2002b), and also supported by the regulators (Bank of Thailand, 2003; Matsushima, 2000; Yakcop, 2000). Even though these changes were planned, the organization was not ready to address and manage the related changes in its information security risk.

To gain an economic advantage and compete better, ALPHA, like many other organizations, took an expansion approach in its business and merged with two other major financial institutions with different specializations, one in the investment banking and equities businesses, and the other in investment and asset management. The merger required ALPHA to integrate organizations and business units of different sizes, practices, skills and expertise, risk tolerance, and risk management principles into a new business enterprise. This also brought new challenges to the IRM function about how to close the gaps, while maintaining compliance with regulatory restrictions and requirements that existed in the different entities, as well as the combined new enterprise.

While these organizational changes were taking place globally, the Internet continued to grow and proliferate as a communication and collaboration vehicle for business and individuals (Furnell, 2002, pp. 1-17; Hall, 2001). Along with this has been an escalation of security incidents relating to software vulnerabilities exploitations (AusCERT, 2002). Since then, the sophistication of attack techniques and motivation
for financial fraud have also increased (Furnell, 2002, pp. 21-39; Skoudis & Zeltser, 2004, pp. 9-13). In September 2001, shortly after the 9/11 incident, a computer worm by the name of NIMDA (CERT/CC, 2001b) caused a massive disruption of email, web, and IT services in organizations (Pethia, 2001). This was followed by the SQL Slammer worm (CERT/CC, 2002b, 2003a; Krebs, 2003) incident in January 2003, and the Blaster worm (CERT/CC, 2003c) incident in August 2003. In the same period, incidents of unsolicited emails (commonly known as SPAM) also escalated exponentially (The Economist, 2003). All this resulted in significant losses and impacted ALPHA’s information security risk status. However, information risk manager’s role and responsibilities were unclear when these security incidents occurred, and most users did not know how to respond when their systems were being disrupted.

These incidents are a form of unplanned changes that resulted from security events that are often beyond the control of the organization. How should information risk managers respond in terms of managing such changing information risk situations?

1.1.2 Common Knowledge, Standards, and Practices

Managing information security risk has been commonly regarded as the task of identifying and assessing risks, applying mitigating controls, and monitoring the use of those controls to address the recognized risks in a coordinated manner throughout the lifecycle of the business system. In the security standards arena, the former British Standards BS 7799 Part 2 (1999b) on “Information Security Management Systems” (ISMS), which has been revised as ISO/IEC (2005f) IS 27001 codified this as a “Plan-Do-Check-Act” (PDCA) process. This standard used baseline controls such as the ISO/IEC (2000) IS 17799 standard for implementation. The controls in these standards were however symptomatic and were categorized broadly to be selected and refined based on the results of the risk assessment process. Their use was therefore subject to individual interpretation relying primarily on the risk manager’s knowledge and experience. However, in a changing business and IT landscape faced with tight budgetary constraints and reduced development time, these security controls, which focused on past known issues, often become internal obstacles when the businesses planned to provide new services to their customers. When the perceived benefits of not implementing security controls were higher than the uncertain or subjective value
of having them in place, the controls would often get ignored, rejected or placed in lower priority for implementation.

There was also a lack of a standard lexicon or taxonomy in information security terminology and practices.\textsuperscript{11} As noted in Jones (2005), this has resulted in many unfavorable implications for the information security profession, with frequent ramifications ranging from “marginalization in the organization, difficulty in convincing organizational leadership to take recommendations seriously, to inefficient use of resources.”

In the area of new IT systems and network communications technology, businesses strive to increase productivity, to reduce the cost of operations and other overheads, or to reach out to more potential and existing customers. Security standards and best practices were often not readily available in time to support the management of risks related to fulfilling such needs, even if the business was willing to invest in protective measures up front. A primary reason was the lack of available best practices due to a lack of relevant security know-how and experiences relating to the new technology and related systems. This resulted in the need for business management and IT practitioners to take risks if they wished to capitalize on new solutions or approaches to solve existing business problems or improve business efficacy. In most cases, security measures that were previously devised for other business contexts and requirements were deployed to secure the new systems and protect information involved. Discrepancies between the new and the old quickly became security gaps that the business had to manage separately. The organization would not want to dismiss the new technology or opportunity as well, given that it might be disadvantaged in its competitiveness or profitability. Relying on a best practices approach therefore has the undesirable effect of keeping the business IT lagging newer developments. How should information risk managers help the organization to respond to the needs of such changing IT and business environment?

In addition to addressing the above challenges, information risk managers need to demonstrate to the business management that the information risks\textsuperscript{12} of the organization have been managed. In other words, she/he must be able to measure the effectiveness or performance of the IRM related activities. Such metrics have been essential for gaining support and resource investment for the IRM function. This should include investing in security processes, training people to be aware of risks and
pitfalls to avoid and the secure steps to take, conducting regular reviews and monitoring to identify security gaps, and address new security issues. Whether these actions have been accomplished however would not necessarily translate into zero security incidents in the organization. These security practices were nevertheless auditable.

The primary approach adopted to measure the effectiveness of IRM in ALPHA, and 30 other participating practitioners’ organizations of this study was to use audit and compliance ratings\textsuperscript{13} of the presence and integrity of the security controls as a primary measurement, followed by a count of the number security incidents. As reviewed and analyzed in Section 2.5.7, the number of security incidents and the security status of an organization has a non-linear relationship. Such an approach, although has its own merits, reflects only a partial view of the information risk status of the organization, and effectiveness of the information risk managers.\textsuperscript{14}

Besides the use of compliance and stability metrics to determine internal performance, some organizations have adopted a benchmarking approach to determine its position against other organizations within their business industry. This approach, however, also has its own limitation, due to cultural, business priorities, and other influencing factors, as discussed in Section 2.5.7.

These issues raised the question of how should the effectiveness of information risk managers, including their strategy and plan, and the risk status of an organization be assessed or measured so that they would provide a more meaningful indication of the organization’s risk exposure compared with current approach of relying on the number of issues identified, and the audit rating of those issues.

1.1.3 Profession, Organizational Role and Function

At a personal level, my interest in information security risk management research relates directly to my practices, in my previous role as a Regional Information Risk Officer (RIRO) for ALPHA, in which this research began, and my current role as the regional Security Advisor (SA) in a technology providing organization (BETA).\textsuperscript{15}

In the role of a RIRO, I was responsible for devising approaches and steps to help the organization manage its information security risk with the purpose of reducing security-related exposures and uncertainties due to the use of IT (including the
Internet) in the organization. In the role of an advisor, I was responsible for providing professional advice to help Information Security Risk Managers and those with related roles in enterprises to develop their security strategy and plans, and manage the execution of those plans to achieve similar objectives such as those that I had in my previous role as a RIRO. Without a practice-oriented approach supported by research, the validity of a suggested information security strategy and plan may be challenged. It was also hard to ascertain that an observable reduction\textsuperscript{16} of security exposures and uncertainties was an outcome of their actions.

The field of information risk management has been an emerging one. It has evolved from the practice of data security to information security protection to management to one that has integrated the risk management discipline. At the point at which this study was initiated, there were still differences between practitioners and researchers as well as within the respective communities about the definition and scope of information risk management. For example, a practicing regional CISO asserted that it is a discipline that evolved from the field of information technology (IT) security and information security (Mahtani, 2004); but Maiwald and Sieglen (2002, pp. 5-10) suggested that the role is contingent to the purpose of the information security department, whether the latter has resulted from government regulation requirements, audit report recommendations, senior management or board of directors’ decisions, or IT department decisions. The literature review in Chapter 2 has also identified five different approaches in the definition of information security, and differences in defining and scoping the meaning of risk management and risk assessment.

At the same time, organizations like ALPHA, which have an information risk management practice, have been re-defining the scope of the function frequently.\textsuperscript{17} Such frequent changes further supported the view that the domain needs more examination and evaluation in order to understand what it entails, and what needs to change in order for practitioners to achieve the IRM objectives.

1.2 Purpose of this Study

The purpose of this study was to identify and establish a suitable approach for managing information risk\textsuperscript{18} in the changing risk environment of enterprise organizations, taking into consideration the issues and dilemmas observed, including
the challenges and questions in the knowledge and practice of information risk management outlined above.

1.3 Research Questions

In line with the background, motivations, and purpose of this study, three main research questions were formulated from the list of questions identified in the practice environment discussed above. These questions provided the basis for the selection of research methodology and structuring of the research process, facilitated the theoretical inquiry about the data, and guided the exploration and development of an approach suitable for use in managing information security risk in an enterprise.

1. What should an Information Risk Manager do differently or change in his/her strategy and plan, in managing information security risk for the organization in order not to result in a compliance driven and/or control-oriented security culture?

2. How should Information Risk Managers manage the information security risk in a constantly changing business and IT risk environment, such as (1) security risk development in the information technology arena that could disrupt the business and/or IT operations, and (2) changes in the business and/or IT strategy and implementation that could significantly change the organization’s risk posture?

3. How should organizations resolve the conflict between the performance measurements of the Information Risk Manager and the outcome of a security incident? Should the Information Risk Manager’s performance reflect the security risk status of the organization, or, in other words, what should the relationship be between her/his performance and the security status of the organization?

As security implementation would incur a cost to the business, and security risk management has to enable the business to balance this cost with the potential gains from its objectives, these questions therefore should be studied in the context of a business environment to ensure that the business objectives are adequately balanced with the information security risk management practices.
As discussed in Chapter 2, these questions about information security risk management have not been adequately answered with current literature and knowledge in the field of information security. More importantly, there have been inconsistencies in the use of terminologies and basic structure and principles for defining and addressing information security risk management requirements, resulting in much confusion to newcomers in the field. It is therefore an important area requiring more studies and understanding in order to refine existing and develop new knowledge, and work towards an acceptable framework, model, and/or approach to evolve and improve the practice. This study, which has a major focus in these areas, will therefore provide significant knowledge contribution to the domain of information security risk management upon completion.

1.4 Research Methodology

The social-technical nature of information security risk management challenges and the exploratory nature of the research questions suggested the use of a qualitative approach for the study. Furthermore, the research questions arose from the workplace, which was an appropriate environment for seeking the desired outcome. Action research, which has been successfully applied by other researchers and practitioners in workplace-related research, for examples, in Goh (1999), Kwok (2001), and Tay (2003), was therefore chosen as the meta-methodology for the conduct of the study, to derive the theoretical approach for information security risk management, and testing its implementation in an organization (CHARLIE).¹⁹

The study entailed identification of the issues and dilemmas in managing information risk, based on the understanding gained in organization ALPHA, and further triangulated through a mini-survey followed by interviewing of 30 other respondents in the industry. An evolving model and associated change programs were developed and implemented to address those issues and dilemmas over four major action research cycles, extending to organizations BETA and CHARLIE. Kemmis and McTaggart’s (1988) “Action Research Planner” was adapted in the initial action research cycles. The action research process was further influenced by the works of Avison, Lau et al. (1999), Dick, Passfield, et al. (2001), Dick (2003; 1993; 2001) and Costello (2003) in subsequent cycles. Data collection included interviews, use of questionnaires, and journaling. Analysis and interpretation of data included evaluation and reflection about the data collected, using both dialectic and systemic analysis of
the findings, leading to a derived substantive theory and approach for information security risk management. The derived approach and supporting methodology and tools were subsequently validated through case studies and test implementation in the practice environments.

1.5 Delimitations of scope and key assumptions

The study began when I was first employed by organization ALPHA, leading to the conceptualization and proposition of a piezoelectric hypothesis for information risk management. Due to a change of employment, to organization BETA, I was unable to carry out an implementation of this theoretical approach in the same environment to fully complete the theorizing process in the same research environment. To overcome this limitation, case studies were conducted in organization BETA to triangulate the data and verify the validity of the derived approach. Questionnaires and interviews were conducted with the senior security executives of 30 other organizations to further triangulate the findings of the initial phase. The data collected supported the piezoelectric approach as the appropriate approach for answering the research questions. A framework for information risk management (FIRM) was also developed based on the research, and implemented in another organization, CHARLIE, in which results were obtained and reported. In spite of the limitation, the research has progressed beyond ALPHA and BETA, with case studies conduct on related security incidents and focusing events, and testing implemented in CHARLIE and two other practical contexts, therefore demonstrating the applicability and possible generalization of the piezoelectric principles and approach to a wider context than that in which the research was conducted.

While the question on the security and risk of outsourcing was raised earlier in the commencement of this project, the study did not focus specifically on this aspect of risk management. Instead, the broader questions of managing information risk associated with constant changes in the business environment emerged as a more important question for this study. Outsourcing, as well as mergers and acquisitions, often resulted in changes to the organization structure and information flow, repositories, and sources of generation, access, and destruction. Consequently, the change of the trust relationship, resulting in organizations needing to trust more third parties to handle business-sensitive and critical information, required information risk managers and people in general within the organization to be responsive. Answering
the question of how to manage information security risk relating to change was therefore one of the objectives of this project study.

Due to resource limitations, and a relatively low maturity\textsuperscript{20} of the field in the Asia region, the survey that was conducted as a method of triangulation and validation was limited to 30 participants. More rigors in this data collection effort were achieved however through the conduct of follow-up interviews with the participants. More rigors to the data, reflections, analysis, and interpretation to support the outcome for the study were also added through the use of open dialogues with fellow practitioners in multiple public conferences, seminars, and roundtables, in which progress of the study was shared and discussed.

Regardless of these limitations and assumptions, the research outcomes have contributed a new substantive theory and provided a new perspective for implementing information security and risk management with the research outcomes as highlighted in Section 1.6.

1.6 Research Outcomes

The outcomes of this study included two set of conclusions; (1) the inadequacies of existing baseline, control-oriented approach and practices, and (2) the proposed method for addressing those inadequacies.

The following inadequacies of the existing approaches and practices in information security risk management, as previously experienced prior to this study, were found to be true in the first three action research cycles in ALPHA:

1. The existing approach of information security risk management practices, which has mostly been baseline controls and compliance oriented, resolved only known security risk at best, and did not prepare the organization systems to respond systemically (as described in Section 3.3.3.2.3) to new and emerging security risk;

2. Such an approach, which relied mostly on instilling fear, uncertainty, and doubt (FUD) about information security risk, have not gained stakeholders’ commitment on the value of information security practices;

3. The use of a baseline compliance status rating system for performance measurement, such as a Red-Angem-Grer (RAG) color-coded Scorecard in
organization ALPHA, did not provide a basis for a systemic—effective, reliable, efficient, meaningful, and fair—evaluation or measurement of the performance of information security risk managers, and the information security posture of the organization that they served; and

4. A baseline controls and compliance oriented approach, as implemented in ALPHA, did not reflect the existence of information risks that were unknown to the organization, did not make systemic provision to address the issues of unknown information risk, and did not learn from the occurrence of resulting unexpected security events. The implication of this was that the organization continued to face negative impact when a significant change took place in the risk environment, even though resources had been invested in information security risk management.

To address these inadequacies, the research study continued through the fourth action research cycle (with two sub-cycles) in BETA and CHARLIE, and concluded that:

1. The existing baseline and risk management approaches should be complemented with social-technical tools and processes to establish and ensure stakeholders recognition and commitment to actions for information risk management. Techniques such as stakeholder analysis (S), entry and contracting (E), dialectic data analysis (D), convergent interviewing (C), and Flood’s (1999) Four-windows system view, were tested suitable for focusing on developing and implementing an information risk management system incorporating a five-level action map and a framework developed to deliver the desired risk management outcomes for the organization; and

2. Managing information security risk in organizations requires focus on the responsiveness of the organization and people to information security risk. In this regards, the study conceptualized a substantive theory of information security risk management, known as the piezoelectric theory. The piezoelectric theory, named after the characteristics of piezoelectric electrical material, states that if the design of information security practices of organization systems enables a prompt re-alignment of the systems, satisfying the systemic requirements for the changing risk condition of the systems environment, the negative effects of the new risk condition of the systems
environment will be balanced or counter-acted by the re-alignment activities. As a result of piezoelectric behavior in organizational systems, as evidenced in this study, the consequences of the emerging or new risk condition of the environment will likely incur a reduced impact to the organization system. Results of the study also showed that the significance of the consequences relates inversely to the security readiness, and thus, responsiveness of the organization. Readiness relates to the organization’s preparedness to re-align its activities and take the appropriate actions to balance against the negative effects of the changing risk environment in a timely and systemic manner.

The validity of the substantive piezoelectric theory was supported by case studies of actual practices in an organization, two significant security incidents, and a focusing event during the course of the study, and tested through the development and implementation of a responsive approach to information security risk management in a participating organization and two other projects.

In addition to the above, the study further established the following outcomes relating to action research:

1. Action research, as a method of inquiry, has enabled me, as a researcher, to observe and reflect from my practice and research study critically and rigorously, leading to the development of the piezoelectric theory, and the development of the responsive strategy and tactics, contributing to the knowledge domain of information security risk management;

2. Action research, as a meta-methodology, has enabled the use of a variety of other inquiry methods and analysis tools suitable for addressing different aspects of the research based on the problems and issues arising at each juncture of the study. This has enabled the research findings and propositions to be triangulated with multiple sources of data and analysis before conclusive outcomes were determined, supporting the research criteria (Section 3.2.1) identified as part of the study; and

3. Action research, as a method of inquiry, has enabled me, as an information security practitioner, to observe and reflect my practice and knowledge critically and rigorously therefore learning from such a method to improve my practice and contributed to management improvement in the organizations that
I have worked through the period. Initial trial of action learning in ALPHA, and ongoing dialectics had also contributed to improve the knowledge and practice of other information risk practitioners in the organization.

1.7 Significance of this Research

As reviewed in Chapter 2, existing knowledge for managing information risk in organizations centered on the concept of baseline controls and general principles of risk management focusing on risk mitigation as a strategy\textsuperscript{23}, but was unable to address the questions (Sections 1.1 and 1.3) identified in this study. This study has confirmed the knowledge gaps and implementation issues relating to the existing approach as practiced in ALPHA, and contributed to the understanding of these issues and the existing approach in the practice environment. The issues identified in this study were also common in many other organizations, as supported by the findings from 30 other practitioners who participated in this inquiry.

The piezoelectric theory of information security risk management derived and developed through this study has provided a new perspective to the problematic issues by casting the organization’s focus on the notion of critical alignment and responsiveness to changing risk situations, addressing unknown security risks through a responsive security strategy, while maintaining a sound baseline practice to address known risks with an extended objective of improving responsiveness.

The piezoelectric theory of information security risk management is thus a major knowledge contribution to the epistemology of information security risk management.

This study entailed the development of an initial framework for responsive information risk management. The outcomes of the research cycles had evolved the initial framework and associated change programs into a substantive management model applicable to practitioners for managing information risk given similar or near similar organizational settings.

The evolved model provides a method to improve certainty in the outcome of information security risk management, therefore enhancing predictability, and improving the overall security posture the organization, i.e., having the information risk managed. This is a significant contribution to the practice.
For managers in a different organizational environment, the outcome of this research will provide valuable insights to study and evaluate their own situations, taking into consideration the different facets and aspects of the practice identified, and enable them to develop their own unique approach based on the proposed model to better manage their IT and business information risk environments.

Additional research outcomes and knowledge contributions are in the areas of how external information security-related events and standards changes will influence the model, as well as how the model may be adjusted to different organizational settings as a general purpose model for information risk management.

The risk management model has integrated action research methodologies, therefore exhibiting knowledge contribution to the development of the action research paradigm in its own right.

This study has also showed how an action research methodology can be applied in inquiring and understanding the information risk management practice, as part of a management framework, creating a knowledge discovery and learning tool for information security and risk management practitioners, and presenting potential pitfalls and caveats practitioners should avoid, thus ensuring effective use of the action research methodology.

From the academic standpoint, there has been a lack of literature and studies on the social-technical aspects of information security risk management. The research contribution from this study is a step forward towards closing this gap. As discussed in the Conclusion Chapter, more studies need to be conducted to further develop the approach into a more detailed model that can be more easily studied in the academic setting, and applied in the practice environment. This will then facilitate the implementation and evolution of the approach into a more generic model suitable for use in a wider range of organizations.

The findings from this research study are thus relevant and applicable to other organizations that share similar experiences.

1.8 Organization of this Dissertation

The rest of this dissertation is organized as follows:
Chapter 2 reviews the current literature relating to the research and practice guidance on information security risk management, including common assumptions and principles involved. The literature review focused on literature relevant to the initiation of this study. Other literatures that relate to the data are discussed as part of the research cycle in the subsequent chapters.

The research methodology used in this project is described in Chapter 3, with justification of its selection and use, including how the rigor and validity of the research and outcomes were attained throughout the study. Chapter 3 also describes the action research cycles and research procedures used throughout this study.

Chapter 4 analyzes and interprets the data collected through the four main action research cycles, in conjunction with the use of case studies, and further findings from other data and knowledge sources that were used to triangulate the results of analysis, as well as to gain further understanding on specific issues identified in the research cycles.

The outcome of the analyses and interpretation of data in final action research cycle was the development of a framework and supporting tools and methods for a responsive approach for information risk management. The components of the framework, strategy and the tactics are also deliberated in Chapter 4, with examples of their usage and implementation in the organization, answering the questions that were raised in the earlier research cycles.

Chapter 5 concludes this dissertation with a summary of responses to the research questions, the study completed, and the final outcomes, including detailed descriptions of the knowledge contribution to the information security risk management knowledge domain. The chapter also discusses the management contribution, and identifies suitable future work to further the development of this knowledge domain and the responsive security strategy and approach developed in this study.
2 Literature Review

2.1 Introduction

This chapter provides a critical review of existing literature relevant to the field of information security risk management. The purpose of this review was to synthesize current knowledge, support the needs, and highlight the significance of this research in the field of information security risk management. The review focused on literature that has informed the knowledge field of information risk management and commonly adopted by practitioners in organizations that either recognized the need for managing information risk, or were mandated by laws or regulations to do so.

In most dissertations, a full review of all literature relevant to the study would be undertaken and reported in this chapter. However, the methodology used in this study – Action Research – is data driven. As such, only literature relevant to the initiation of this study was included in this chapter. Literature relating to the data was reviewed as part of the research cycles and reported in the chapters that follow.

The review began with an overview of the concepts, including definitions and principles of information security, risk, risk management, and information security risk management, as described and discoursed in the current literature. The review then focused on the strategies and programs for achieving information security in organizations. The theories and knowledge expounded by current literature in the context of the concepts, strategy, and programs for managing information security risk were reviewed against the key characteristics – change and potential security failures – of the information security environment, which were the key themes underlying the research questions discussed in Chapter 1.

The review conducted for this chapter included published work found in academic research journals, books, conference proceedings, and related articles and discussions from the trade press, journals, magazines, security forums, conferences, and seminars, including online versions of these materials. Keyword searches for specific terms such as “security”, “information security”, “information risk”, “risk assessment”, “risk analysis”, “risk management”, “information security management”, “security management”, information risk management, and “information security risk management” were performed on ACM Digital library, Southern Cross University’s
online databases, IEEE online digital library, and the National Library of Singapore, where relevant publications were reviewed as part of the study.

2.2 Information Security

It is often said that information security is not new (Hoo, 2000, p. 2; Piper, 2006), however, several definitions of the term “information security” have been developed and used in both the academic and business world. In many ways, this has shaped the scope and approach towards achieving information security. For the purpose of this chapter, a review and understanding of the definitions is therefore presented.

The historical development of information security can be traced back to the ancient use and development of cryptography (Kahn, 1996; Singh, 1999), in which protecting the confidentiality of information was the main focus. Data and information confidentiality have also been the primary concern of national defense and intelligence, which initiated early development of security models, such as the then widely used Bell and La Padula’s (1976) model. As understanding of information communications developed and evolved, in particular, in the business use of information technology, and progress in information technology demonstrated that protecting the integrity of information is also critical to ensure the authenticity, correctness and accuracy of information contents, and authenticity of the sender and recipient, new models for information integrity protection began to emerge, for example, the Biba Integrity Model (Pfleeger, 1997, p. 280), Clark and Wilson (1987) and subsequent works of Abrams, Amoroso, LaPadula, Lunt, and Williams (1993).

Beside cryptography, access control has commonly been used to achieve integrity and confidentiality protection, by ensuring the authorization of a user against the access matrix of a protected resource or information (D. E. R. Denning, 1982). Denning (1982) also introduced the notion of information flow controls and inference control for protecting the confidentiality of information in transit and stored in database systems, respectively. When these security mechanisms are enforced to achieve information confidentiality and/or integrity, unauthorized users will be blocked from accessing that information. However, if the security mechanisms are forcibly disabled or damaged, a perpetrator will be able to remove the availability of the information protected from the authorized users, preventing its use when it is most needed. From this, it became clear that availability is another important requirement in information
security protection. Clark and Wilson (1987) were among the early researchers who highlighted the need for availability, in particular, in business systems.

A common definition of information security has therefore been the protection of information to ensure its confidentiality, integrity, and/or availability, e.g., see Shain (1994), Hoo (2000), and Blakley, McDermott, and Geer (2001). Over the years, practitioners and researchers have also invested much work in clarifying the meanings of these terms, which led to expanding the basic definition of information security to also include authenticity, accountability, and, in some cases, usability. One of the most elaborate expansions of this definition was in Parker (1998), which included authenticity, possession, and utility as extensions to the list of security properties desired. However, confusion prevailed in the field. For example, Clark (2003, pp.: 23-24) defined security differently in different parts of his book, and included trust, privacy, non-repudiation, and integration (without elaboration) as parts of the definition in one instance (see D. L. Clark, 2003, p. 33), whereas Maiwald and Seiglein (2002, pp. 5-10) suggested that the role of information security was contingent to how the function originated in an organization, which dictated its mission and objectives. In this case, the definition of information security will rely on the individual or organization’s views and beliefs. However, Maiwald (2004) also defined information security as “measures adopted to prevent the unauthorized use, misuse, modification, or denial of use of knowledge, facts, data, or capabilities”.

While this definition has added “capabilities”, “knowledge”, and “facts” to the meaning of information security, it has excluded the confidentiality or privacy requirement.

In view of the lack of agreement on and consistency in the list of information properties in the definition of information security, members of ISO/IEC 17799 revision working group adopted a different approach when the “Specification for the Code of Practice for Information Security” (ISO/IEC, 2000) was revised in 2005, and redefined information security as “the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities” (ISO/IEC, 2005e). This approach emphasized the relationship between information security and business, highlighting the need for information security to be aligned to business objectives.
In Alberts and Dorofee’s (2002, p. 5) description of the OCTAVE\textsuperscript{SM} approach,\textsuperscript{24} “information security is determining what needs to be protected and why, what it needs to be protected from, and how to protect it for as long as it exists”. In essence, this definition framed information security as a process to identify information assets, prioritize the importance of each asset, understand the threats to the assets, and devise suitable measures to protect the assets against threats. In other literature, this process has been known as risk analysis and risk management. For example, see Pfleeger (1997, pp. 462-471), Moses (1994), and Summers (1997, pp. 616-629).

Another approach, as Alberts and Dorofee pointed out, was to answer the question of “how to assure your organization an adequate level of security over time”.

Volonino and Robinson (2004) also emphasized the importance of gaining assurance, but took a law-oriented approach, including considerations relating to the different parties involved in the conduct of a business transaction electronically. They defined information security as

the policies, practices, and technology that must be in place for an organization to transact business electronically via networks with a reasonable assurance of safety. This assurance applies to all online activities, transmissions, and storage. It also applies to business partners, customers, regulators, insurers, or others who might be at risk in the event of a breach of that company’s security (Volonino & Robinson, 2004, p. 1).

The various ways in which information security has been defined showed that the scope of information security, as a knowledge field, encompassed many aspects of information and information systems. Synthesizing the existing literature, there are at least five distinct areas to be considered in order to address this topic comprehensively:\textsuperscript{25}

1. Information security properties or attributes, such as confidentiality, integrity, and availability;

2. Policies, processes and functions, from information creation to destruction;

3. Priorities or criticality, as a function of the threat and regulatory environment, their potential impact on the business, and available resources within the business;
4. Techniques or measures applicable to address security requirements or issues; and

5. Assurance to verify and validate the completeness and effectiveness of the security measures taken to provide the security properties, secure or support the processes and functions, and address the priority threats and regulatory requirements.

The relationships between these areas and the context of their identification, assessment, implementation, operations, and maintenance need be relevant to the business. In addition, there is a need to evaluate and relate how information security in an organization will address changes in the business environment, in particular, adverse conditions that emerge as a consequence of changes and failures in the environment.

However, with the except of a few studies, such as Dhillon and Backhouse (2000), most literature have been focusing on specific methods and techniques to respond to changes and issues that have already taken place, or well known, but not in anticipation of and be prepared to respond to emerging changes. In other words, most studies were more concerned about understanding the past and present, and devising solutions that would help to manage and address issues that had been encountered previously, but not on developing models and approaches that would deal with ongoing changes and the future. A study undertaken in the actual practice environment is therefore an important step in addressing this question from both the technical and sociological perspectives.

2.3 Principles and Approaches

To achieve the objectives of information security covering the five areas highlighted in the previous Section, different approaches and methods have been devised and implemented. (Appendix C provides a synthesis of the main approaches in relation to the five categories of definition discussed in the previous section.) To help in determining the appropriate approach and method, researchers and practitioners have over the years used a number of basic principles in the design and development of information security systems.

Swanson and Guttman (1996, p. 1) referred to those principles “as certain intrinsic expectation [that] must be met whether the system is small or large or owned by a
government agency or a private corporation”. As part of this review, this chapter discusses and analyzes four fundamental principles that have been widely used in information security management, and the approaches that have been largely influenced or based on these principles, namely: (1) the weakest link; (2) defense in depth; (3) no perfect security; and (4) risk management. For discussions of additional security principles, see Swanson and Guttman (1996), Schneier (2003), and Summers (1997, pp. 7-9).

2.3.1 Security is only as strong as the weakest link

“A chain is no stronger than the weakest link.” … No matter how strong the strongest links of a chain are, no matter how many strong links there are in it, a chain will break at its weakest link. Improve the strength of the weakest link and you improve the strength of the chain. (Schneier, 2003, p. 103)

This metaphoric principle has been widely cited in information security literature suggesting the need to consider all aspects—people, process, and technology—and not to focus only on one or a few particular areas as a reaction to a recent adverse incident or legal, regulatory, or audit requirement.

When identifying the weak links in a system, Schneier (2003, pp. 103-104) highlighted that different threats often have different weak links. Countermeasures designed to counter a weak link therefore would not work for all threats on the system. For a more detailed discussion and examples of the use of the weakest link principle, see Browne (1972, pp. 1, 3), Denning and Denning (1979, p. 228), Schneier (2003, pp. 103-116) and Viega (2005, p. 44).

As noted in Browne (1972, pp. 1, 3) “it is important to be systematic and come up with interlocking measures that prevent or recover from nearly all types of contingencies”—proposing the need for a “fortress” of security, and supported by the “defense in depth” principle.

2.3.2 Defense in depth

Defense in depth is about “protecting assets with not one countermeasure, but multiple countermeasures” (Schneier, 2003, p. 105). By overlaying or complementing each countermeasure, a security weakness at a lower layer will then be secured by the protection rendered at the higher layer(s), and vice versa.
When devising layered security solutions with the defense in depth principle, information risk practitioners have commonly suggested looking into people, process, and technology aspects of requirements. Howard and DeBlanc (2003, p. 19), and Schneier (2001, p. 370; 2003, pp. 103-117) also cited the weakest link principle as the basis for implementing defense in depth to reduce the surface area of attacks in software products and application systems. From a detective perspective, such a principle helps to increase the probability that an attack will be detected earlier, when detective mechanisms are placed at each layer. The provision of redundant and backup security mechanisms were also considered as implementing defense in depth (Pfleeger, 1997, p. 404). For example of the use of this principle in practice, see Microsoft Corporation (2006b, p. 46).

While weakest link and defense in depth are sound principles for reducing vulnerabilities, and providing layers of defense to overcome unexpected problems, they will increase the cost of security with each layer of security added to the systems. As reported in Venables (2004), the increased layers of security will also add complexity to the environment. Such complexity will result in emergent behaviors, creating new, unanticipated weak links and making security more difficult to manage.

### 2.3.3 Use of security technology

Historically, a common research approach in computer security has also been to identify weaknesses and possible attacks, and to devise techniques and mechanisms to protect against them. As such, when addressing information security risks, it has been common for some groups to regard information security as a technology problem, and that “given better access control policy models, formal proofs of cryptographic protocols, approved firewalls, better ways of detecting intrusions and malicious code, and better tools for system evaluation and assurance, the problems can be solved” (Anderson, 2001b). As noted in Blakley, McDermott, et al.: 

Information security is important in proportion to an organization’s dependence on information technology. When an organization’s information is exposed to risk, the use of information technology is obviously appropriate (Blakley et al., 2001).

Even when considering social requirements, the tendency has been to translate them into technical measures for implementation. For example, Kohl (1995) stated that “the problem of security is drifting from technological security, whose main interest lies in
the sound calculation and possible certainty about the non-human world, towards an area of human relationships which are technologically induced, so that the aim of security is becoming once again a state between humans”. To address these needs, Kohl proposed a set of technical security mechanisms providing for “information self-determination”, “non-repudiation”, “reproducibility”, and “design potential” for the end-users (Kohl, 1995, p. 613).

Technology vendors have also been favoring such an approach for several reasons besides the obvious business motivation. For example, Kluepfel (1994), BizNiche (2006), Cisco Systems (2007) and others have suggested that building and using security technology would provide better integration of security with technology, eliminate the need to deal with human procedures that can be error-prone, and lower the cost of security. Similar thoughts appeared to also prevail in the end-users’ organizations (Allen, 2002).

While such an approach towards information security has resulted in many technological innovations (for example, anti-virus, firewalls, intrusion detection, and intrusion prevention systems), in themselves, they can hardly claim victory over the changing risk environment, in particular, on the Internet.

For one, security features that were designed for specific security requirements became difficult to change when the business needs or policies changed. For example, security mechanisms such as security label, mandatory access controls, object reuse, and many others that were specified in the former Trusted Computer System Evaluation Criteria (US-DoD, 1983, 1985) were fixated towards meeting the various levels of security in the military security policies defined according to the Bell-LaPadula security model (Bell & LaPadula, 1976). These security mechanisms, when implemented in computer systems, cannot be used in commercial businesses without having the businesses aligning their security policies to those of the military and defense, which is quite impractical. Similarly, while a firewall system is able to block undesirable network traffics on pre-determined network ports, it is ineffective to deal with application-level attacks that were executed using legitimate network services, tunneling through authorized network ports that the firewall system allowed. An application-level security mechanism will have to be devised and implemented in addition to the firewall in order to deal with newly identified risk. Security features that are designed to cater to a wide range of requirements often become too complex
to manage or configure (requiring additional tools and skills), or could not address specific needs comprehensively and still perform within reasonable efficacy measures.

Volonito and Robinson (2004, p. 55) also noted that such an approach has been problematic as “it often gets defeated by faulty configuration of the tools, neglected maintenance, or a process failure, such as the failure to close out the network IDs [access identifier] of terminated employees”. In addition, “it shows little senior management commitment; has no specific economic justification; [and] requires little to no active participation from employees”. Similar issues in various aspects of information systems and network implementations were also discussed in Kang (1996), Schneier (1997; 2001), and others, emphasizing the potential human errors in the information system lifecycle, and highlighting the need to also focus on people, policies, and processes for implementing and managing information security.

As also noted in Blakley, McDermott, and Geer:

Current information security technology, however, deals with only a small fraction of the problem of information risk. In fact, the evidence increasingly suggests that information security technology does not reduce information risk very effectively (Blakley et al., 2001).

Blakley, et al., therefore argued “that we must reconsider our approach [of using security technology singularly] to information security from the ground up if we are to deal effectively with the problem of information risk”.

Nonetheless, reporting on the PricewaterhouseCoopers and UK Department of Trade and Industry’s (DTI) April 2002 survey results (2002), J. H. Allen highlighted that “people still look at security as a technology issue, when it should be a business matter” (Allen, 2002: citing comments from Etienne Greeff). In 2004, after a follow-up survey, the UK DTI reported that “some progress had been made in putting security controls in place”. However, most of these were focused in technology-related solutions. As summarized in the PriceWaterhouseCooper and DTI report:

Businesses tend to rely solely on their firewall to defend their Internet gateway and web-site against attack.

Fewer than one in ten businesses (and only a quarter of large ones) have tested their disaster recovery plans to see if they would work in practice.
Neither overall awareness of BS 7799\textsuperscript{28}, nor the number of UK businesses that have implemented it, has increased over the last two years.

Spend[ing] on information security, while increasing, is still relatively low and is seen as a cost rather than an investment.

Companies now spend on average 3\% of their IT budget on security compared with 2\% two years ago. Large businesses spend roughly 4\%. Overall levels of investment in security are still considerably below the 5\%-10\% benchmark level.

Under half of all businesses evaluate return on investment on security spend[ing].

(PricewaterhouseCoopers & DTI, 2004)

As shown in these reports and studies, while the use of security technology has the potential to provide for defense in depth with its deployment across the infrastructure layers, it was normally not achieved. Due to cost and other resource constraints, organizations have the tendency to rely on a single security technology to address multiple security needs. As such, even if people and processes were adequately secured, potential weak links would still exist at the technology layer due to non-technology reasons. The use of security technology singularly therefore have not fulfilled the needs of the weakest link principle.

2.3.4 Baseline security

Building upon the strength of using available security technology, addressing the concerns of vendor-driven solutions and the lack of focus on softer issues such as people, processes, and policies, the baseline approach has taken a more comprehensive view by setting up a minimum level of security, with little attention to cost,\textsuperscript{29} that must be implemented across all information technology systems and infrastructure in the organization (Summers, 1997, pp. 6-7).

The use of baseline security was common between the 1980s and the early 1990s, when businesses began to deploy information technology, with increasing dependency on its security. This involved establishing standards of best practices that were acceptable among all organizations in a similar industry. Through the use of baseline standards, Ferris (1994) added that an organization could establish “a framework of tools for deciding acceptable risks, and acceptable social behavior”. The baseline approach was formalized and published as an international standard, ISO/IEC Technical Report 13335 (ISO/IEC, 1999), as a method suitable for managing IT
security in organization. In terms of specific security measures to be implemented, a number of standards have also been developed by industry and international organizations—for example, the BSI’s BS 7799-1 (BSI, 1999a), and ISO/IEC 17799-1 (ISO/IEC, 2000, 2005e) standards. The U.S. Department of Defense “Trusted Computer System Evaluation Criteria” (TCSEC) (US-DoD, 1985) was also considered to be one of the baseline standards, and was used in the U.S. government in establishing a standard-based policy to achieve better assurance and a measurable level of security (Ferris, 1994), addressing different levels of needs with a set of pre-defined classes of security (Summers, 1997). Although it was based on a set of security policies, it used technical security measures as the main approach towards addressing the policy requirements. TCSEC has since evolved into the Common Criteria, and become an international standard, ISO/IEC 15408 (ISO/IEC, 2005b, 2005c, 2005d), articulating security features and their measurable assurances in computer systems. The standard defined the process by which different industries with computer security needs can craft their own variations of security standards, called “protection profiles”, with the aim of providing for more flexibility for each industry.

The baseline security approach, which was also known as the “checklist approach” (Dhillon & Backhouse, 2001), involved the following high-level steps in managing information security:

- Use of checklists (as a risk assessment tool) to identify security requirements and issues;
- Defining acceptable policies and standards;
- Implementing standards-based solutions across all systems;
- Using a combination of technology and procedural measures;
- Use of compensating controls to address new issues until a technical control is available to close the gap (identified from the checklist review); and
- Security reviews and audits as assurances of compliance and implementation – based on the use of checklists.

The main criticisms of the baseline approach were the omission of a continuous risk analysis and assessment process as part of information security management, and
increasing the cost of security across the organization when non-critical business and information assets were also accorded the same set of baseline measures. The latter was known to result in undue administrative overheads when non-compliance with baseline measures about non-critical business or information assets were raised in audit reviews, since, from an audit perspective, if a common baseline has been included as part of the company’s policy, non-implementation of any of such baseline, even for non-critical assets, would be considered a non-compliance issue. This approach therefore has a side-effect of driving compliance instead of ensuring adequate management of information security risk. Compliance has in fact been a strong driver of information security in most companies. According to Sullivan (2006), in a survey conducted by Merrill Lynch & Co. Inc., in 2006, responded by 50 chief information security officers, regulatory compliance topped the list of reasons driving demand for security software.

Ferris also commented that

One shortcoming of the policy [of using a baseline standard across his organization] was its lack of emphasis on the importance of establishing an information security policy, which is critical to the successful implementation of discretionary access control. This is a critical management issue, but not a technical one (Ferris, 1994, pp. 75-76).

To reduce the cost of security controls, Venables (2004) proposed establishing a “high universal baseline”, and to focus on solutions and component integrations to “make it easier to do security than not to”. A reduction of the cost of security, however, has not been shown possible with a high universal baseline. Setting a high universal baseline will nevertheless add cost to non-critical assets, or assets that are not handling or storing any critical or sensitive information, and cost of additional security administration and monitoring.

According to Dhillion and Backhouse,

The [baseline] checklist approaches, although still widely used, carry less conviction when searching for theoretical foundations in security. They indicate where exclusive attention has been given just to the observable events without considering the social nature of the problems. Checklists inevitably draw concern onto the detail of procedure without addressing the key task of understanding what the substantive
questions are. Procedures are constantly changing and for this reason offer little in the way of analytical stability. (Dhillon & Backhouse, 2001)

From a legal perspective, according to Hoo (2000, p. 11), “the basic premise [of a baseline best practice approach] is that conformance to a set of best practices will ensure protection against negligence-based liability lawsuits in the event of a security breach”. However, Volonino and Robinson (2004, p. 193) commented that baseline best practices are not necessarily recognized by the courts as the standard providing a sufficient defense. That is, best computer security practices for an industry may not be an effective defense for a company if those practices can be shown to be substandard or outdated.

The term “best practices” has been a common source of disagreement amongst practitioners and researchers. At the 2003 CRA Workshop on Research Related to National Security, McKeown, Clarke, and Stankovic (2003) reported that “the security subgroup had the least agreement on what constitutes best practices, opting for the term ‘plausible practices’ instead”. At the launch of the first “BS 7799 Goes Global” conference in Singapore, Humphrey (2002) also highlighted that “best practices, in reality, are common practices”. Standards such as BS 7799 have eased the selection of security measures, and provided a “common language” for information security practitioners when discussing security risks and safeguards. They have been used to improve information security, but ultimately need to be part of the organization’s risk management system, in support of its security policies and requirements.

With the changing IT environment, whereby digital communications and connectivity have increased exponentially with widely available access to IT systems, Ferris also recognized that “IT security standards have to evolve along with the technical environments that they serve”.

This new environment requires flexibility in adjusting to, or adding on, new technical applications and assessing the risk impacts. Reliance on technology for new control functions in terms of integrity (e.g. electronic signatures) and access control (e.g., privacy) has increased dramatically (Ferris, 1994, pp. 75-76).

To meet the changing requirements, Ferris suggested a “security services orientation, with services requiring a tool box of standard IT security products to support the services” and to provide alternative techniques for satisfying IT security requirements,
giving system planners better choices, and empowering decision makers to determine the balance between cost and risk acceptable to their organization (Ferris, 1994, pp. 75-76). In other words, instead of a common set of baseline standards and security measures, a wider set of alternative security standards were required to support different needs. The questions of how to determine needs and decide which standards to use was paramount in such a multiple baseline standards approach.

These shortcomings of the baseline approach imply the continued existence of weak links in the systems, and multiple baselines mean additional cost and complexity in implementation, similar to the issues in a defense in depth approach.

2.3.5 No Perfect Security

Another generally accepted principle is that of “no perfect security”, based on the notion that information systems involve human actions, and a human is not a perfect being. In the world of cryptography, the notion of “no perfect secrecy” has been well known. The “One-time Pad” (D. E. R. Denning, 1982, pp. 86-87; Singh, 1999, pp. 120-124) data encryption technique, for example, was therefore designed to achieve perfect secrecy, which, however, was too expensive for any practical use. Despite variations of the One-time Pad being used, they have only been deployed in highly sensitive systems such as those involving national security, with trade-offs in terms of significantly reduced convenience of use, increased cost of implementation and use, and accepting the risk that the cryptosystem might be breakable under certain conditions. In other words, allowing certain “weak links” in the systems.

McKeown, Clarke, et al. also reported in the 2003 CRA Workshop on Research Related to National Security that:

Best practice is often limited …, which are often decades behind the techniques put forth by the research community. This dichotomy between research and practice in security means that different recommendations must be developed for different situations. Given that all of our systems have vulnerabilities, it is unrealistic to expect that any system can ever be entirely secure (McKeown et al., 2003).

In essence, the “no perfect security” principle countered the principles of weakest link and defense in depth. It requires the risk manager to take a more pragmatic approach when implementing the defense in depth principle, accepting the notion that weak links will be present regardless of the number of layers of defenses used. Essentially,
the risk manager has to “trade-offs” between risk and available resources, which is the basis of “risk management” (Schneier, 2002; 2003).

2.3.6 Information Security is Information Risk Management

Recognizing the wisdom of “no perfect security” and the need to prioritize and decide resource allocations within a limited budget for security expenditures, a risk management approach is therefore logical, and widely proposed as the approach for managing information security.

Also known as a “cost-benefit approach” (Summers, 1997, p. 6), Denning and Denning (1979, p. 228) suggested that “the goal is cost-effective internal safeguards, sufficiently strong that computer hardware and software are not the weakest links in the security chain”. Swanson and Guttman (1996) has similarly stated that the requirements for risk management in two computer security principles, namely “computer security supports the mission of the organization”, and “computer security should be cost effective”.

Blakley, McDermott et al. (2001) rationalized that since information security has been concerned with the protection of business-critical or sensitive information, and related IT systems and infrastructure, failures of information security would mean the occurrence of adverse events, resulting in losses or damages that therefore has impact on the business (negatively). As such, information security has to be a risk management discipline involved in managing the cost and/or impact of information risk to the business. In other words, “information security is information risk management” (Blakley et al., 2001).

While adopting a risk-based principle for information security appeared sound, and often highly recommended—for examples, see Alberts and Dorofee (2002), Clark (2003), Schneier (2003), PriceWaterhouseCoopers (2003), and the Electronic Banking Group of the Basel Committee on Banking Supervision (2003)— there are challenges in adopting all the principles concurrently to address the needs of information security.

2.3.6.1 Risk, Risk Assessment, and Risk Management

Risk has been known as the “possibility of incurring loss, injury, or harm” (Manser & Turton, 1987), the “possibility of suffering harm or loss” (Alberts & Dorofee, 2002, p. 8), a “combination of the probability of an [adverse] event and its [negative]
consequence” (ISO, 2001, p. 12), or simply “being exposed to the possibility of a bad outcome” (Borge, 2001, p. 4). Possibility meant an element of chance (or probability); and loss has often been associated with the value of an asset, which might be tangible or intangible, such as reputation. As such, risk has often been associated with hazards to valuable assets.

The combined process of identification, analysis and evaluation of asset value, threats, vulnerabilities, attacks, exploits, and impact has commonly been known as a risk assessment.30

According to Borge, “risk management means taking deliberate actions to shift the odds in your favor—increasing the odds of good outcomes and reducing the odds of bad outcomes” (Borge, 2001, p. 4). Risk management has also been known as “the ongoing process of identifying risks and implementing plans to address them” (Alberts & Dorofee, 2002, p. 8). ISO (2001) defined risk management as “a set of coordinated activities to direct and control an organization with regard to risk”. Risk management has therefore included risk assessment, risk treatment,31 risk acceptance, and risk communication.32

2.3.6.1.1 Assessing Risk

In ISO Guide 73 (2001, p. 16) “risk analysis” is defined as the “systematic use of information to identify sources and to estimate the risk”.

Risk analysis provides a basis for risk evaluation, risk treatment, and risk acceptance. Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders (ISO, 2001, p. 16).

Risk analysis has commonly been conducted using qualitative methods (using classification such as low, medium, and high as risk measurements), although business management would often prefer quantitative risk measurements in order to enable numerical comparison with other financial analysis for decision-making purposes.

Qualitative risk assessment methods have ranged from the use of simple “low/medium/high” characterization of the probability and consequences of risks, to complex formulae that have included the use of expert systems, but achieved very limited success. CRAMM33, and RISKPAC34, for examples, were fairly widely used commercial risk assessment tools that employed the qualitative approach in the 1990s
(Moses, 1994, pp. 250-263). In the late 1990s and early 2000s, with the proliferation of the Internet and related risks, more technical methods such as “Penetration Testing” (Klevinsky, Laliberte, & Gupta, 2002; Maiwald & Sieglein, 2002, pp. 46-49; Tiller, 2003), “Threat Modeling” (Howard & LeBlanc, 2003, pp. 69-124; Schneier, 2001, pp. 288-306), and “Scenario Analysis” (Hoo, 2000, p. 11) have emerged as newer tools for conducting qualitative risk analysis and assessments.

Qualitative risk assessment has been more common in enterprises, due mainly to dissatisfaction with quantitative methods. As noted in Moses,

> There was a need to be able to properly identify values of data assets in relation to the potential effects of impacts that were really impossible and illogical to present purely in financial terms, for example, endangerment of personal safety, and to assess the level or likelihood of threat source manifestation and level of seriousness of vulnerabilities without subjective specification of frequency of occurrence and other figures (Moses, 1994, p. 250).

The validity and reliability of qualitative risk assessment methods are, however, also subjective, and often rely heavily on the experience, knowledge, and rigor of the risk analysts.

Quantitative measurements provide a sense of “authoritative, confident-sounding expressions of uncertainty” (Adams, 1999, pp. 23-24). In information risk literature, quantitative risk analysis has often measured potential losses using “annual loss expectancy” (ALE), computed as a function of the “annual probability of loss” (p) and the “value of the asset” (v). That is,

$$ALE = pv$$


ALE was proposed by the U.S. National Bureau of Standards (1975) as “Federal Information Processing Standard (FIPS) 65”. While the standard was withdrawn in August 1995, it continued to be a well cited approach for quantitative risk assessment. Hoo (2000, p. 12) attributed the appeal of ALE metric “in its combination of both risk components [probability of loss and value of asset] into a single number”. This “blending” was however also a major disadvantage, since distinguishing high-frequency, low-impact events and low frequency, high-impact events could no longer...
be made from a single number itself. Making a decision based on the ALE alone can therefore become risky, since a high ALE number due to the former can be tolerable, whereas one due to the latter may be catastrophic (Perrow, 1999, pp. 306-328).

To simplify the risk computation, some quantitative methods eliminated the probability of loss. Those methods, which Hoo (2000, p. 18) named “Valuation Driven Methodologies”, and one of the “Second Generation Approaches”, used only the valuation of the assets and potential impact in the risk computation, which allowed the risk managers to “focus on issues of managerial acceptance, institutional inertia, and other deployment issues”. Hoo, however, added that:

Although attractive for their simplified approach and avoidance of controversy, these valuation-driven methods suffer significant theoretical flaws by virtue of that same simplification. Their exclusive focus on asset value and ignorance of safeguard costs, efficacy measures, and frequency of security breaches could result in either over-securing assets or under-securing them. Both possibilities are economically inefficient and could cause competitiveness to suffer. Without the capacity for performing cost-benefit analysis or the requirement of basic statistics collection, these methods provide no mechanism to motivate refinement of their security specifications. Although convenient in the short term, valuation-driven approaches are not viable long-term solutions (Hoo, 2000, pp. 18-19).

Evolving from the learning of the ALE approach, researchers have been promoting a more expanded view of risk assessment, which Hoo described as a “common framework” approach, which considered the security requirements (R), assets (A), security concerns (C), threats (T), safeguards (S), and vulnerabilities (V) when deriving a risk assessment outcome (O). Such a framework was to promote an iterative assessment process that included a series of threat analysis, safeguard selection, and cost-benefit analysis. The method could be used for both qualitative and quantitative risk analyses. Several commercial software implementations of the framework have also been made available, for example, @Risk, and CRAMM, with varying degrees of popularity. According to Hoo, “throughout the 1990s, sporadic research efforts in computer security risk models can be found, and despite the best efforts of those involved, the framework and other ALE-based approaches failed to gain widespread acceptance”. Hoo assessed that the methodology failed due to three main flaws:
1. Mismatch between the method, which is scenario based, and the task of mathematical or computer modeling, which affect its accuracy when it aims for simplicity, but become overly complicated and impractical if they consider all possibilities;

2. The model requires a deterministic problem space, “assuming that all quantities [are] precisely known”, but not on a probabilistic scale. “The inability to recognize and capture uncertainty handicapped risk modelers”.

3. The model requires, and assumes, all information—frequency, valuation, and efficacy data—are available. Such data, however, remains largely unavailable.

What followed in Hoo’s review was a mixture of the development of risk management and risk assessment, which was inconsistent with the initial focus of his analysis. Hoo’s categorization of the “second generation approaches” included the “Integrated Business Risk Management Framework”, “Valuation-Driven Methodologies”, “Scenario Analysis” Approaches”, and “Best Practices”.

Hoo commented that

“The new approaches tend to focus almost exclusively on solving the deployment and organizational acceptance issues that plagued the earlier ALE generation, thus leaving the challenges of complexity and uncertainty unaddressed (Hoo, 2000, p. 17).

This appeared to be so, as Hoo has combined risk management and risk assessment as similar tasks, which was inconsistent with his initial review, which covered only risk assessment. The scope of risk management is much broader than risk assessment. Risk management encompasses risk assessment as part of the management process. From a management perspective, addressing deployment and organizational acceptance issues is therefore within the scope of any risk management framework. As reported by Barton, Shenkir et al. (2002, pp. 13-14), scenario analysis and self-assessment using checklists were commonly used as part of the overall risk management system in the risk identification process. In addition, best practices approach has been in use in the U.S. government and a number of multi-nationals companies since the 1980s, as discussed in Section 2.3.4, prior to the practice of risk management, and continued to be used through the 1990s into the 21st century. In line with the synthesis of the literature conducted in this review, Hoo was however

34
accurate in stating that “the challenges of complexity and uncertainty [has remained] unaddressed”.

Summarizing his review, Hoo noted that

Most of the new and innovative work is hidden behind a veil of corporate secrecy, rendering a full exposition and analysis of the second-generation approaches unachievable (Hoo, 2000, p. 17).

This observation has again highlighted the need for real-world practices of risk management in the field to be evaluated and reported.

The four new approaches to managing risks are, in general, short-term solutions to the problem. Although they have been relatively successful in addressing organizational acceptance and deployment issues, they have left largely untouched the technological and informational challenges of the previous-generation methodologies. Their lack of cost justification, inability to forecast future trends, and disregard for safeguard efficacy measurement will impel organizations to seek a more satisfactory, quantitative framework for managing computer security risks (Hoo, 2000, p. 20).

Notwithstanding the limitation of the ALE approach, Blakley, McDermott et al. (2001) commented that:

Security technology development and selection should be based on quantitative observational studies of effectiveness, not on synthetic a priori assurance of vulnerability avoidance. Probabilities of exploitation must be balanced with consequences. ALEs (that is, observed outcomes) must rule, not the emotion of a good story and the fear, uncertainty and doubt that continues to be the selling proposition for most security technology (Blakley et al., 2001).

Denning (1999, pp. 388-389) also reported concerns over the validity of quantitative risk assessment methods, and many information security experts believed that it was not practical to get a degree of exactness about risk.

Risk assessment is not an exact science. It is impossible to estimate precisely the likelihood of an attack or the losses that would be incurred. There are many potential adversaries—hackers, competitors, criminals, foreign governments, terrorists, and so forth—each with different motivations and skills and each having a different impact on the target. Vulnerabilities are not always known until they have been exploited, and security mechanisms can have costs that are too hard to quantify or predict in advance (D. E. Denning, 1999, p. 386).
Even though the weaknesses and limitation of a quantitative risk assessment approach were profound and such a method was not well accepted and implemented in practice, Hoo evaluated the approach of risk management undertaken in the insurance and liability risk industry, and concluded that

insurance, liability, and competition are underlying forces that will push computer security risk management away from the non-quantitative, second-generation approaches and back toward a quantitative framework of risk assessment and management similar to the first-generation ALE-based methodologies.

Given this assumption, “a new approach is needed, tempered by the lessons of the past and capable of adapting to the future demands that these forces will soon thrust upon it” (Hoo, 2000, p. 20).

At the Computing Research Association (CRA) Conference on “Grand Challenges in Information Security and Assurance” held in November 2003, a risk management approach to security was identified as one of the important challenges facing the field. The conference again emphasized the need for quantitative risk measurement rather than leaving the approach more open, even though it was clearly stated that there was a lack of understanding of the full nature of what causes IT risk, the emergent behavior of some vulnerabilities and systems, and dependencies in the failures of networked systems. Specifically, the “Grand Challenge” stated that:

Within 10 years, develop quantitative information-systems risk management that is at least as good as quantitative financial risk management (Computing Research Association, 2003).

The bias towards a quantitative measure of risk (at the CRA Conference and in general) was fueled by the notion that “we cannot manage if we cannot measure”. The CRA Challenge conference, however, also emphasized that “what you measure is what you get”, and that “measuring the wrong thing is as bad, or [is] worse than not measuring anything at all”; and the need for the measures to be consistent, unbiased, and unambiguous. The main questions that the CRA Challenge posted were:

How much risk am I carrying? Am I better off now than I was this time last year? Am I spending the right amount of money on the right things? How do I compare to my peers? What risk transfer options do I have? For that matter, they have no corresponding ability to match their efforts to warning levels such as Yellow, Orange, or Red (Computing Research Association, 2003).
The last point is in fact the most crucial, as it relates to emerging or changing risk situations that organization has faced. Even if the five questions can be answered accurately and fully substantiated with multiple charts and graphics of quantitative measures, the inability of an organization to deal with an escalating risk situation will result in damages and losses, making all earlier efforts and measurements irrelevant.

From the risk communication perspective, Gigerenzer (2002) also found that the use of probabilities did not help to facilitate risk communication. Instead, Gigerenzer suggested that “when thinking and talking about risks, use frequencies rather than probabilities”. Gigerenzer asserted that frequencies have provided more clarity of the risk involved through the use of a reference class. Such an approach, however, was not known to be used in information security risk analysis.

While quantitative methodologies have received a much higher emphasis and continued to gain the interest of current researchers, studies on qualitative approaches remain limited. This was attributed to the technical focus of the field of information security. In order to gain a better understanding and develop new knowledge on qualitative methodologies in risk analysis and assessment, qualitative, empirical studies in information risk management, like the work of Bjorck (2005), are also important, and should be encouraged.

2.3.6.1.2 Managing Risk

While risk analysis seeks to identify and evaluate the significance of risk to information assets in organizations, risk treatment resolves to determine appropriate actions (or non-actions) for those risks identified and evaluated.

Blakey, McDermott, et al. (2001) suggested that “risks can be managed using a variety of mechanisms, including liability transfer, indemnification, mitigation, and retention”. In accordance with the definition of risk management, for example, ISO Guide 73 (2001), these mechanisms were more commonly known as risk treatment mechanisms.

In risk treatment, organizations have been overly biased towards the use of mitigation in comparison with other approaches, even though the number of insurance companies offering the option of using liability transfer and indemnification has been increasing (Blakley et al., 2001; Gordon, Loeb, & Sohail, 2003; Hoo, 2000).
Blakley, McDermott, et al. noted that the lack of risk data, including data on vulnerabilities, incidents, and losses, was one of the main problems of using liability transfer or indemnification approaches for risk treatment. As also noted in Hoo (2000, p. 29), “practical implementation issues aside, no consensus yet exists on the specific quantities to be monitored, as evidenced by the distinct lack of consonance among computer security surveys”.

The notion that insurance has provided a means for liability or risk transference is however flawed. As noted in Boyne (2003, pp. 3-22), in the insurance business, risk is taken from the perspective of potential of loss to the business, but not the customer (people or organization) being insured. In terms of managing such a risk, the insurance company looks at the history of risk events relating to the profile of the individuals being insured. A premium is then established based on the probability of the occurrence of a similar past accident to the insure. In this way, the insurance company will be able to collect substantial premiums with the lowest chance of a payout. Aggregation has also been practiced so that the collective amount will be much larger than the potential payouts that the company will need to incur in case of a mishap, or multiple mishaps taking place around the same period or same time. From the insuree perspective, subscribing to an insurance scheme therefore does not actually transfer her/his risk. It only provides a means for a limited recoverability when something has gone wrong, i.e., when she/he is exposed to a condition or event that results in substantial loses, including the potential loss of life. When using an insurance policy in the field of information security risk management, the same principles apply. The risk therefore remained.

Gordon, Loeb, and Sohail (2003) also reported that the use of insurance to address information risk issues was still in its infancy. Faced with challenges and concerns over issues such as “adverse selection” and “moral hazard”, insurance companies were still uncertain about how to price their products. As such, relying on using insurance to manage risk has its own risk. In the framework proposed, Gordon, Loeb, et al. maintained the importance of risk assessment and understanding of the company’s risk tolerance as a key determinant of the appropriateness of an insurance policy.

Risk mitigation meant the use of security measures, including the implementation of technology or processes, with or without the addition of new human resources, to
Chapter 2 – Literature Review

protect the system, information, or environment against the identified risks. This has usually taken the form of controls, by removing or disabling “risky” features and functionality, often resulting in the crippling of the usability of information systems, in order to mitigate (or rather, eliminate) the risk identified and assessed to be significant. As such, mitigation measures were seldom welcomed by business or end-users, and often seen as a form of productivity impediment. Risk mitigation typically involved the use of best practices baseline security standards – such as the ISO/IEC 17799 (2000; 2005e) standard – to address known risk issues, and implementation of technical security measures wherever possible to ensure secure use of specific technology, and/or automate the mitigation into the organization’s work flows and processes. A vast number of publications, both online and in print, have provided for this requirement. For examples of mitigation measures, both technical and procedural, see Pfleeger (1997), Garfinkel and Spafford (1997), Summers (1997), Potter and Fleck (2003), Meier, Mackman, et al. (2003) Egan and Mather (2005), Hellen and Goetz (2004) and Maiwald (2004), just to name a few. For issues that did not yet have technical solutions, additional procedural measures were normally devised as temporary compensating controls.

In risk acceptance, or risk retention, the evaluated risk is tolerated, or retained. Such a decision was often due to the perception that the probability or the impact of the downside was so insignificant that ignoring the risk was acceptable. If an organization has tolerated a risk, it would need to be financially prepared to sustain the impact of its occurrence (Degraeve, 2004, pp. 49-50). The financial industry (in which ALPHA was one), being a highly regulated industry, however, has a very low appetite for risk and uncertainty—risk that cannot be quantified or estimated and assigned with a probability value. As such, risk acceptance was seldom a viable option, even if there was a documented procedure for accepting risk formally in the organization.

2.3.6.2 The problems of a risk-based approach

A risk-based approach, despite its benefits, like the other approaches discussed earlier, has numerous challenges and issues as well.

2.3.6.2.1 On risk terminologies

Risk-related terminologies—threat, vulnerability, attack, adverse events, impact, crisis, and danger—are often used loosely, and at times, in confusing ways that do not
differentiate one from the other. For example, in describing the changing risk
environment as a result of new technology and security attacks on the Internet, Egan
and Mather (2005, pp. 11-12) used phrases such as “blended threat” and “rapid spread
of these threats”, when discussing the new attacks, and commented that “the threats
are expected to continue to grow”, when it was the probability of occurrence that
could potentially grow, but not the threat itself, which consequently escalates the risk
of doing business on the Internet. When an information risk manager conducts a risk
assessment, it is at times unclear whether she/he is assessing threats, attacks,
vulnerabilities, or the risk *per se*. The mixing of the terms risk assessment and risk
management was also evidenced in Hoo (2000) in Section 2.3.6.2 when the two topics
were reviewed.

### 2.3.6.2.2 On probabilities

In analyzing the driving safety and seat belt policies in the United Kingdom, John
Adam (1999) commented that the probability of loss in the context of a risk
assessment was different than the probabilities relating to the throw of a pair of dice.
Unlike dice, information risk events were not necessarily deterministic, and the
outcome of information risk was also not independent of previous or other risks (or
throws). As such, if we were to apply statistical measurement of risk, we would need
to collect and analyze information about previous similar events, and then extend the
past statistical trend into the future to arrive at a predictive judgment. As noted earlier
in Blakley (2001) and Hoo (2000), there has been a lack of data and consensus in data
formats to permit an accurate statistical measurement of risk. Even if these constraints
were resolved, there would still be issues with regard to the use of statistical data. As
highlighted in Levinson, issues in the quality of data, sample size, population
involved, and expertise of the risk assessor, would impact the conclusions of the risk
assessment in various ways:

> Reaching conclusions about an entire population from the statistics of a sample is like
> enlarging a photograph. Small defects are magnified into serious blemishes. If a
> sample does not take proper account of the classes that make up the population it is
> supposed to represent, it is called a biased sample.
>
> But the failure of a sample to take account of all possible distinctions by no means
> proves that it is a biased sample. It is only the omission of essential distinctions that
> renders a sample inadequate, and it is not always evident in advance which
Chapter 2 – Literature Review

characteristics will turn out to be essential. This indicates a fundamental difficulty against which the statistician (and the critic of statistics) must be continually on guard. In a sense he cannot know with certainty how to collect the data for his sample until his investigation is in an advanced stage. He may find, for instance, after exercising every precaution that his data contain some unknown disturbing factor, and this may be due to the failure to separate in his sample two classes that should have been separated.

When the statistician is himself in control of the collection of the data for his investigation, the difficulty is not insuperable, although it may mean a large added amount of labor. But when he is forced to use data collected by others, perhaps for entirely different purposes, and possibly years ago, he is in danger of finding himself with a hopeless statistical problem on his hands. All this requires the soundest sort of judgment, for which no amount of technical mathematical skill is an adequate substitute. On the other hand, the statistician with a defective knowledge of higher mathematics will find that the technical aspects of the subject absorb an undue proportion of his attention and energies, to the detriment of his handling of the investigation as a whole. If he has no knowledge of higher mathematics, he is incompetent and has no business to conduct a statistical investigation.

In addition to the danger of reaching false conclusions due to a biased sample, there is the danger of reaching equally false conclusions because the sample is too small. (Levinson, 1963, pp. 206-207)

Boyne added that “if neither a priori nor statistical measurement of risk is possible, we are forced to resort to ‘estimates’” (Boyne, 2003). When a risk issue was estimated to have a profound impact, the risk would likely be given a higher rating. Adams remarked that “when risks become perceptible, when the odds are publicly quoted, the information is acted upon in ways that alter the odds“ (Adams, 1999). The accuracy of the quantitative risk analysis would therefore become subjective. The subjective nature of risk analysis would likely result in incorrect assessment, leaving weaknesses (or weak links) in the system with a false sense of security.

2.3.6.2.3 On the risk of risk analysis

Charette (1991) commented that “the premier risk in doing any risk analysis is that the recommendations for the management of the risks reached are inaccurate”. An overestimation of risk would cause an excessive amount of mitigation effort—beyond what was truly required—to overcome the perceived risk. On the other hand, an
underestimation of the risk would likely result in a false sense of security and undesirable surprises, often coupled with management panic about how to react to the unplanned consequences. In either case, confidence in the risk assessment and recommendations would be affected in subsequent analysis. Ironically, if a risk analysis was highly accurate, the true value of the analysis would also be subverted, since the risk would have been effectively managed and consequently, no adverse event or losses would result. Justifying more resources or continuation of the risk management activities would subsequently not get the appropriate management attention. Risk analysis has also been misused in organizational politics in order to resist change and keep the status quo, and also as form of blame analysis, becoming a form of intimidation instead of a means to improve the situation (Charette, 1991).

Adams argued that

risk is a continuously reflexive phenomenon; we all, routinely, monitor our environments for signs of safety or danger and modify our behavior in response to our observations—thereby modifying our environment and provoking further rounds of responses ad infinitum. [As such,] the act of measurement alters that which is being measured (Adams, 1999, pp. 23-25).

As potential events, not certainties, risk has no quality control. The value of the analysis therefore could not be ascertained (Charette, 1991).

2.3.6.2.4 On the cost of risk analysis

Charette (1991) and Summers (1997, p. 616) further noted that “risk analysis has its own costs”, which included the cost of software tools, and the time and expenses incurred by the risk analyst in completing the analysis. Despite finding that “the results are imprecise and lack empirical validation”, Summers, citing Perry (1985) and Baskerville (1991), commented that

risk analysis is worth doing, even when not mandated. It provides insight into security and improves security awareness, and sometimes it is the only way to justify expenditures on security. Risk analysis gives managers a familiar kind of information—measures of costs and potential gains and losses (Summers, 1997, p. 616).
2.3.6.2.5 On risk identification and perception

In many ways, the media, including press and television, has also played a significant role in providing risk information, in the form of influencing the perception of the stakeholders and other opinion providers, including the risk analysts. However, as highlighted in Boyne (2003, p. 29), “when the media tell the public about risks, they will do so in relatively simple terms, based on official and attributable sources, reducing access damage to their channels of support as far as reasonably possible; and they will do all this in such a way as to maximize sales”. The proliferation of the online and print media has therefore introduced additional risk and uncertainty to the risk analysis process.

2.3.6.2.6 On management

According to Magretta (2002), management, as a discipline in the business arena, has been regarded as the most important innovation of the past century.

Management makes organizations possible; good management makes them work well. … Management’s business is building organizations that work. … Underneath all the theory and the tools, underneath all the specialized knowledge, lies a commitment to performance… Organizations are changing dramatically, and they are taking new forms but, without organization of some sort, nothing would get done (Magretta, 2002).

Drucker (1973, pp. 39-40) cautioned that “bureaucracy, a management that has come to misconceive itself as an end and the institution as a means, is the degenerative disease to which managements are prone and especially those managements that do not stand under the discipline of the market test”.

In the context of information security risk management, there were limited studies and literature on the management and organizational aspects of information security risk, in particular, from Drucker’s perspective of preventing bureaucracy.

Most literature, such as Alberts and Dorofee (2002), Stoneburner, Goguen, and Feringa (2002), and standards, such as ISO/IEC 13335-1 (2004), and ISO/IEC CD 13335-2 (2005) focused on the techniques and mechanics of conducting risk assessments. More relevant work on the management aspects of information security risk management that have been discussed and studied more recently revolved around a system for information security risk management, commonly known as an
information security management system (ISMS). For examples, BSI’s BS7799-2 (1999b), Bjorck (2005), and ISO/IEC IS 27001 (ISO/IEC, 2005f), which addressed mainly the mechanics for implementing and operating a risk management process in the organization.

The underlying motivation for risk management remained as an approach for prioritization and allocation of limited resources to gain the highest returns, leaving aside issues and problems that were seemingly insignificant to the business or the organization. While focus on efficient utilization of resources on significant risk areas were critical, the overall performance of information risk management should not be limited to just this.

Blakley, McDermott, et al. have also reported the lack of studies and discourse relating to the issues and challenges in managing information security, such as people, organization, structure, resource allocation (including financial resources), and performance.

We also know very little about the effectiveness of the measures we take to prevent adverse events or alleviate their consequences. The people to whom these events happen have few incentives to report them; conversely, they have many incentives to suppress information about them. Finally, the system we are attempting to protect (roughly composed of the global Internet and everything attached to it) is far too complex to be understood in detail (Blakley et al., 2001, pp. 100-101).

Essentially, the existing approach of risk management would leave certain issues and risks as they are, based on the result of risk assessment and business priorities. These issues, and related risks, may also be assessed inaccurately and therefore run the risk of becoming the weakest link in the system.

Anderson (2001a, pp. 489-511) summarized the issues from the perspective of security engineering relevant to the business organization:

Risk management may be one of the world's largest industries. It includes not just security engineers but also fire and casualty services, insurers, the road safety industry and much of the legal profession. Yet it is startling how little is really known about the subject. Engineers, economists, actuaries and lawyers all come at the problem from different directions, use different language and arrive at quite incompatible conclusions. There are also strong cultural factors at work. For example, if we distinguish risk as being where the odds are known but the outcome isn't, from
uncertainty where even the odds are unknown, then most people appear to be more uncertainty-averse than risk-averse. Where the odds are directly perceptible, a risk is often dealt with intuitively; but where the science is unknown or inconclusive, people are liberated to project all sorts of fears and prejudices. So perhaps the best medicine is education. Nonetheless, there are some specific things that the security engineer should either do, or avoid. (Anderson, 2001a, p. 492)

Anderson concluded that the issues relating to information security risk management “are amongst the most important—and most difficult—of any in our field, but receive little attention, because they lie at the boundaries with software engineering, applied psychology, economics, and management”. This further supported the needs for this study, which was aimed to identify or develop suitable approach to address the questions of information security risk management from the social-technical perspective in an organizational context.

2.3.7 A Circular Problem

The above analysis of the four common security principles showed that they have a circular connection, all returning to the original problem of the weakest link where the analysis started, as shown in Figure 1.

![Figure 1: The Circular Problem of Information Security Principles](image)

As such, the problem has not been solved by these principles. Current approaches that were based on these four principles without considering the circular problem were therefore inadequate in addressing the needs of information security, and the fundamental issues of weakest link.

To achieve progress, new approaches should not add to the circularity of current principles. This should be one of the criteria for assessing the quality of newly proposed principles for addressing the information risk management challenges, beginning with the outcomes of this study.
Chapter 2 – Literature Review

2.3.8 IT Security Governance

With incidents such as the collapse of the Barings Bank (BBC Online, 1999; Degraeve, 2004, pp. 68-69; Leeson, 1996; RiskGlossary.com, 1996; Stock Market Crash! Net, 2005) and Enron (Bazerman & Watkins, 2004; RiskGlossary.com), “legislatures, statutory authorities, and regulators have created a complex array of new laws and regulations designed to force improvement in organizational governance, security, controls and transparency” (Brotby et al., 2006). With new regulations such as the Sarbanes-Oxley Act of 2002 (Moeller, 2004), non-compliance have impacted not just the organization as a business, but also resulted in the personal liability of the executive officers responsible. As noted in Byrum, “the presence of a strong IT security control structure is crucial to Sarbanes[-Oxley] compliance”.

Without it, management will have to either disclose a significant deficiency in the corporate internal control structure or expose the organization’s executive officers to personal liability in the case that they certify inaccurate financial statements. While the legislation may not have been specifically written to address IT security controls, as compliance efforts progress, the impact of the Sarbanes-Oxley Act on IT security will be substantial (Byrum, 2003).

Coupled with the growing threats of information system disruption and information security breaches from hackers and terrorists, the need for a governance approach to information management has therefore been widely recognized. For example, the Basel Committee of Banking Supervision stated in a 2003 report:

Because the Board of Directors and senior management are responsible for developing the institution's business strategy and establishing an effective management oversight over risks, they are expected to take an explicit, informed and documented strategic decision as to whether and how the bank is to provide e-banking services. … Effective management oversight is expected to encompass the review and approval of the key aspects of the bank's security control process, such as the development and maintenance of a security control infrastructure that properly safeguards e-banking systems and data from both internal and external threats. It also should include a comprehensive process for managing risks associated with increased complexity of and increasing reliance on outsourcing relationships and third-party dependencies to perform critical e-banking functions (Electronic Banking Group of the Basel Committee on Banking Supervision, 2003).

The IT Governance Institute further stated that:
Whilst senior executives have the responsibility to consider and respond to the concerns and sensitivities raised by information security, boards of directors will increasingly be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organizational resources (Brotby et al., 2006).

The Institute proposed five basic outcomes of information security governance, and among them, has included risk management as one of the key outcomes.

The governance approach helps to place information security emphasis at the right level of the organization, giving the information security manager an appropriate mandate to drive his/her programs and initiatives. Within this approach, understanding information risk management, and having a suitable strategy to devise and implementing appropriate programs for execution and implementation are key success factors for delivering the objectives of the governance model.

Our review of the motivation for the risk management principles and current knowledge in the field, however, showed that there were inadequacies in the current information risk management discipline. The inadequacies would result in weak links that could be subjectively assessed as low risk issues, potentially jeopardizing the governance of information security.

The governance approach has brought security to the top management level, giving it the highest level of attention required. This, however, has also created another challenge for the risk managers. Most senior management have a limited time span to discuss risk management issues, and therefore required all details to be summarized to short paragraphs, within a single page or two, and presented with graphics/charts in quantitative formats wherever possible. Risk managers would therefore be driven to eliminate uncertainties and improve “performance”, based on the quantitative figures, with a tendency to focus on showing returns on security investment, improvement in security-related scorecards (or dashboards), and related scores, such as the number of audit issues and security incidents, and the status of mitigation. Compliance and controls would again be keys to “improve” the values captured in those quantitative matrices.

As reported in a recent survey conducted by Ernest & Young LLP (2005, p. 5), 81% of the respondents rated “complying with corporate policies” as one of the most important information security functions. The question of whether such an
improvement in quantitative measures will translate into improved information security in organizations however has not been answered in the current literature. Vijayan (2005) has also reported that corporate security executives have expressed similar concerns about this development.

The literature review conducted in the area of risk assessment showed that quantitative (as well as qualitative) measures were not ready to provide accurate measurement of risk. Based on the studies conducted by Adams (1995; 1999), Boyles (2003), and Lupton (1999) discussed in earlier sections, quantitative measures will always have limitations, and risk measurement will be subjective, due to the effects of risk perception and risk compensation. The field therefore needs more studies to devise better approaches for addressing the issues and dilemmas of information security, and/or managing the related risk. Specifically, this confirms the needs for studies to address the following thematic questions:

1. What should an Information Risk Manager do differently or change in his/her strategy and plan, in managing information security risk for the organization in order not to result in a compliance driven and/or control-oriented security culture?

2. How should Information Risk Managers manage the information security risk in a constantly changing business and IT risk environment, such as (1) security risk development in the information technology arena that could disrupt the business and/or IT operations, and (2) changes in the business and/or IT strategy and implementation that could significantly change the organization’s risk posture?

### 2.4 Information Security Risk Management Strategy

While risk management is to identify significant risk areas and to prioritize and allocate resources for resolutions, and baseline controls and security technology are to address specific concerns that have been identified, they have been tactical and task-oriented, but not strategic. According to Vincent LeVegue,

The basic design of a strategy involves a situation, a target, and a path. … The situation for an information security strategy is the organization’s current environment, consisting of the current technology and management environment. …
The target for an information security strategy is the desired management system (organization structure, staffing, reporting relationships, policies, and procedures) and the desired technical system (computing devices and networks). The path for an information security strategic plan is the set of project plans designed to advance from the current state to the proposed future state (LeVegue, 2006, pp. 1-2).

“Strategy enables us to quickly make the right decisions so that we do not simply react” (Gagliardi, 2004, p. 18). In information security risk management, a management strategy is therefore necessary for developing the information security program or plan (discussed in Section 2.5) and help in deciding suitable actions when faced with contentious risk issues.

In the current literature, the concept of information security risk management strategy has not, however, been widely discoursed, but loosely used in some literature when describing specific action plans or programs—for examples, see APEC-TEL (2004a) and PriceWaterhouseCoopers (2003).

Strategies may be defensive or offensive. Consideration for the use of offensive strategy in achieving information security, in particular, in business organizations, has been very limited, for examples, Information Warfare (D. E. Denning, 1999; Kittler, 1998), and the use of a bounty program (Monica, 2003). The focus of this study was on defensive strategies. Two fundamental strategies commonly known were: (1) Protect-Detect-React; and (2) Detect-React-Protect.

### 2.4.1 Protect-Detect-React (PDR)

In practice, a common, “de-facto”, strategy that has shaped the thinking of information risk managers most frequently in devising their plans was that of “Protect-Detect-React” (PDR) model, which comprised the following high-level steps:

1. First, seek to *protect* the information resources against the identified risk, mainly through prevention or avoidance of attacks, and/or reduction if not elimination of vulnerabilities, by controlling the behavior of the system and/or people involved.

2. Next, seek to *detect* unauthorized behavior or activities in and around the system, including people using and administering it, mainly through
Chapter 2 – Literature Review

monitoring and regular security and log/audit trail reviews, penetration/vulnerability testing, and/or observation of executions to identify human or system-identifiable unacceptable behavior or patterns. Detection may be used either as an additional layer of security (as in defense in depth), or as a compensating measure when there was no deployable protective measure against the vulnerability identified.

3. Finally, prepare to react or respond when an undesirable event has been detected, or has occurred. In practice, this was commonly provided by including two main tasks in the information security plan, i.e., incident handling and management, and business continuity planning and disaster recovery.

The PDR strategy for managing information security has been widely accepted, with a few variations used in the practice environment. For example, Microsoft (2006a) defined “Plan-Protect-Detect-Respond” as the four strategic categories, and Doll, Rai, and Granado (2003, pp. 77-118) used “Restrict-Run-Recover” to re-group the tasks of PDR as the “Three Rs of Digital Security”.

2.4.2 Detect-React-Protect (DRP)

From a timeliness perspective, Schwartau (2001) assessed that the PDR model, if executed in the sequence of 1) protect, 2) detect, and 3) react, would only provide adequate security to the organization if the amount of time required for the protective measures to be overcome was greater than the total time for detection of a security breach, and the time period before the security team has reacted to the problem. In other words, the following equation must hold true, and then the organization could be secured:

\[ Pt > (Dt + Rt) \]

where \( Pt \) denotes the protection time; \( Dt \), the detection time; and \( Rt \), the reaction time.

On the other hand, if \( Pt \) was less than \( (Dt + Rt) \), the difference would provide the perpetrator a time gap to compromise the system or information asset without being detected or time for a reaction to it. This would result in damage or losses that would impact the organization.
Chapter 2 – Literature Review

Given this finding, Schwartau suggested re-sequencing the PDR model as 1) detect, 2) react, and 3) protect (DRP), or “Time-based Security”, placing more emphasis on detection and reaction over protection. If the organization has the ability to detect and react to a security event promptly, even without protection, a security incident would be prevented or avoided. This, from a cost perspective, may result in significant savings, since the cost of protection may be reduced or eliminated. However, the additional cost for devising and implementing a timely detective and reactive security system may be significant.

In a review conducted on an earlier edition of “Time-based Security” (Schwartau, 2001), citing a number of previous publications, Cohen (1998) commented that the idea of using time as a metric to measure security was not new, but nevertheless an important element to evaluate security. Cohen, however, expressed reservations about the assumptions used in Schwartau’s assertions.

On placing higher emphasis on detection:

Detection has its own problems, the chief one being that detection can never be done perfectly in practice. There are always false positives and false negatives and detection takes time. Even if we had perfect and instantaneous detection, our ability to effectively respond is limited by the fact that we don't know how to do appropriate response based on the situation and response itself takes time (Cohen, 1998).

On equating the cost of security to time:

It seems clear that if we are to measure time in terms of money, we need financial models of situations. This in turn requires a system of modeling in which the model changes as dynamically as the environment it models. The model must be fed financial and security information on an ongoing basis and the set of prevention, detection, and response capabilities must be adapted with time to meet the changing business environment (Cohen, 1998).

Citing the military classic—“The Art of War”—by the renowned Chinese General Sun Tze, Gagliardi emphasized that it was not possible to have a perfect strategy, since there would always be new challenges.

We must also understand that no position is perfect for meeting every challenge, and there is no position that does not degrade over time. There is no ultimate victory that ends the strategic struggle. There is no final resting place where everything is perfect.
No matter how far we advance, we will always be confronted with new challenges (Gagliardi, 2004, p. 19).

Similarly, although the four elements—protection, detection, reaction, and time—that have been identified in current literature are not perfect, they are nevertheless important elements to be considered and assessed in devising a security plan. At the minimum, they provide a useful starting point for developing a successful security strategy.

2.4.3 Need for Strategic Thinking

In addition to the general PDR and DRP strategy models, practitioners like Venables (2004) and Wang (2005) have also reported their enterprise-specific strategies for managing information risks in their respective organizations. Venables observed that “security is an emergent property of a complex system”, and suggested that we rethink and change the strategy and approaches based on the theory of complexity.

Wang attributed the constant failure of organizational security programs to the lack of strategic thinking and formulation of business organization-specific security strategy that was often not aligned with the business strategy.

These enterprise-specific initiatives, which evolved from the practice, signaled the lack of strategic thinking in the information security risk management literature. As also noted by Yourdon (2002), in the aftermath of the 9/11 tragedy, increased proliferation and convergence of IT, rapid changes in IT and related risks, and globalization, there was a need re-evaluate existing approaches to risk management from multiple strategic perspectives, and to effect a necessary paradigm shift in order to continue to achieve the objectives of business.

2.5 Information Security Program

In line with LeVegue’s (2006, pp. 1-2) concept of a “path”, as part of the strategy, the information risk manager needs to develop an information security program to implement the selected approaches to achieve the objectives of information security for the business. Also known as an information security plan (Bhagyavati & Hicks, 2003), or a “corporate information assets protection program” (Kovacich, 2003, pp. 95, 125-164), the information security program was an integral part of the information
security strategy providing a blueprint for achieving the information security objectives in the organization.

Synthesizing current literature, seven major areas have been considered in an information security program, namely: (1) organization and people; (2) risk assessment and management; (3) policies; (4) communication, for awareness, education, and training; (5) development, including design of applications, systems, and products; (6) operational security, including administration, monitoring, response, and recovery; and (7) performance measurements.

### 2.5.1 Organization and people

The mission and vision of the organization determine the design of the organizational structure and roles and responsibilities of the ISRM function. The line of reporting, and hierarchical layers between the ISRM function and senior executive management also influence over the amount of authority and span of influence of the ISRM function on the rest of the organization. The ISRM function may be centralized, or decentralized. The former means the establishment of a core corporate-wide ISRM function providing information security risk management as a service to support various businesses and divisions in the organization. In such a structure, the ISRM function may report to the Chief Information Officer (CIO), Chief Operating Officer (COO), or Chief Technology Officer (CTO), or equivalent appointment in the corporate organization. In the latter, decentralized, structure the ISRM function operates as part of individual business and support functions in the respective divisions, with only a small strategic group at the corporate level providing coordination and standardization support to ensure consistent policies and practices among business groups. For a more detailed discussion of the various forms of information security organizational models, including samples of mission statements, and roles and responsibilities, see Dorey (1994, pp. 36-42), Kovacich (2003, p. 166), Kowalski (1995) Maiwald and Sieglein (2002, pp. 5-18), and Summers (1997, pp. 566-568).

Both organizational models, and a combination of centralized and decentralized control, have their benefits and challenges. However, there were limited accounts of how these models would influence the practices of information security risk managers, the strategy and approach of managing information security risk in organizations, as
well as the state of security of organization in practice. More importantly, discussions about security organization models in the literature reviewed seldom considered the implications of the rapidly changing risk environment, as well as more current issues such as merger-acquisitions, outsourcing, and the changing IT landscape, that were characteristics of organizational changes during the period of this study.

People are often regarded as one of the weakest links in the security chain. This applies to people as users, operators, developers, and managers of IT systems and information assets, as well as people in the information risk management function itself.

Besides the need to improve security awareness and competence of people in organization in general, Blakley, McDermott, et al. (2001, pp. 101-102) pointed out that the lack of formal education and professionalism was one of the key issues challenging the information risk management profession. While a professional certification scheme—i.e., the Certified Information Systems Security Professional (CISSP) certification—has existed since the late 1980s, there have been no licensing requirements for information risk manager, and no obligation to report important risk incident or information to a proper authority. Blakley, McDermott, et al. suggested that the inclusion of a “broader and integrated view” for risk treatment to improve the competence of information risk managers. This has given rise to further questions relating to how information risk managers should learn and keep their knowledge up-to-date and relevant, in particular, in a rapidly changing risk and organization environment, which, however, has not been adequately addressed in the literature.

2.5.2 Risk assessment and management

As discussed in Section 2.3.6.1, risk assessment and management has been one of the key topics attracting numerous studies, but at the same time raising more questions, given the issues and dilemmas highlighted in Section 2.3.6.2. This topic has therefore been the main focus of this study.

2.5.3 Policies

Information security policy has been highly emphasized by many as one of the critical elements for achieving information security in organizations (Shain, 1994, p. 5; Whitman, 2003, p. 92). The existence of a security policy has been deemed as
fundamental in an information security program. For example, in the U.S. government, existence of security policy has been used as a measure of the security maturity of government departments (NIST, 2000). Security policies have also been a frequently asked question in most security surveys—for example, AusCERT (2002; 2003; 2004; 2005), PriceWaterhouseCoopers and DTI (2002; 2004), Bogolea and Wijekumar (2004) and Whitman (2003) all considered policy as one of the key indicators of the security posture of organizations and industry.

Although the term “policy” is widely used, it did not have a clear and unambiguous definition. “Policy” may be used to mean a broad orientation, an indication of normal practice, a specific commitment, or a statement of values. … That the term is so widely used suggests that the idea of “policy” has a wide appeal, which leads to its being mobilized in a range of social settings (Colebatch, 2002, pp. 7-8).

In the field of information security, “security policies define the security philosophy and posture the organization takes, and are the basis for all subsequent security decisions and implementations” (Whitman, 2003). 53 Dorey (1994, p. 32) further stated that in a commercial organization, policies “provide a mechanism where the directors and senior management can lay down a clear statement of direction and ‘rules’ for the successful operation of the company”. If created and implemented correctly, they would help to “define security requirements, allocate responsibilities”, and would contribute towards the development of security measures and the control environment.

Guidelines and templates for writing information security policies have also been widely available—for example, see Dorey (1994, pp. 32-35), which also clarified the differences between policy, procedures, guidelines, and standards; and Wood (1995), which provided policy templates to encourage re-use to establish consistency of policy statements.

In practice, however, frequent policy failures have been identified as a key issue. Control Data Systems (1999) attributed them to organizations’ failure in recognizing the four key factors of security, namely: (1) if not designed and managed appropriately, “security is a barrier to progress”; (2) “security is a learned behavior”; (3) “expect the unexpected”; and (4) “there is no perfect mousetrap”.

With numerous “ready-to-copy” policy templates have been available—for example, Wood (1995)—for quick adoption, it has become easy for risk managers to take a
short-cut approach to policy development, bypassing the conduct of risk assessment to ensure that the appropriate policies were developed to address specific risk. Once policies have been published, many were also reluctant to change, as the process involved has often been long and tedious. There has also been a “problem of keeping up with the increasing rate of change in technology or applications”, and also a “problem of keeping up with the increasing rate of change in technology or applications” (Rees, Bandyopadnyay, & Spafford, 2003).

To address the issues of policy failures, life-cycle approaches, which “sees policy as a logical succession of steps” (Colebatch, 2002), have been proposed. For example, Control Data Systems suggested a three-stage life-cycle—(1) “formulation and maintenance”; (2) “enforcement”; and (3) “assurance”; Rees, et al. (2003) proposed a “Policies Framework for Information Security” (PFIRES), incorporating four distinct stages—Assess, Plan, Deliver, Operate.

Rees, et al. suggested using the PFIRES life-cycle approach to “facilitate[s] communications between senior management and technical security management”, and for the organization to be “better positioned to successfully achieve its objectives”. Rees, et al., however, recognized that “much work remains to be done in this area”—in particular, relating to “international and regional concerns, organizational behavior, legal issues, supply chain factors, and industry-specific concerns”. These were “a few areas that would benefit from an in-depth exploration of related information security policy”. Rees, et al. further recommended conducting more research into “how well the life cycle meets the policy management needs of today’s organizations and what improvements need to be made to ensure future success”.

A “social construction” perspective on policy, which differed from the life-cycle approach, saw it as “something that has to be constructed and sustained by the participants in circumstances where they are likely to have choices about which interpretive map to use, which cues to follow”.

It draws on work in a range of the social sciences – sociology, social psychology, organizational analysis and the ‘governmentality’ approach deriving from the work of Michel Foucault – all of which ask ‘what makes for collective action?’, and see this as the question to be answered (Colebatch, 2002, p. 4).

In a rapidly changing information risk environment, with people’s behavior and actions having significant influence and impact on the outcome of addressing security
issues, such an approach towards policy construction and evaluation justified further evaluation. The attributes of policies included “order, authority, and expertise”. Policies would limit choices. Policies also formed the basis for “interrogating organized activities” (for example, in auditing and enforcement of policies). The outcome and process of policies were both important (Colebatch, 2002) to be considered as part of the information security program.

Traditionally, the need for performance measurement in information security has been de-emphasized by having information security requirements captured in corporate policies. For example, Shain found that:

In practice, resources are invested in safeguards only when there is a net return when measured against organizational goals—whether such goals are chosen or imposed (the latter usually by law or regulation). The need to allocate resources for security controls implies that each organization should understand what it is that should be protected, and why. The answers will determine the choice of protection strategy and this thinking should be captured in security policies generated by management (Shain, 1994).

When policies were mandated by senior management, they became part of the business requirements. As policies, they were seldom challenged, even though the policies might be ineffective (Colebatch, 2002).

However, relying on policies to drive information security objectives was inefficient and inadequate.

Policies and regulations were static measures and procedures established for addressing known security risks. If a perpetrator attacked a system, she/he would look for the weakest link in the information security chain, often exploiting a new vulnerability or weakness that current policies, regulations, and/or other protective measures have not addressed, have left out or have ignored. At the same time, the weakest link would not necessarily be known to or addressable by the risk manager or auditor. Even if they did have a method to keep up-to-date on the latest known vulnerability, there was no way of knowing that the known vulnerabilities were the most up-to-date, since the finder might not want to report it publicly (Arora, Krishnan, Nandkumar, Telang, & Yang, 2004).

Time and effort required to effect policy changes to match new or evolving security needs in the changing business and risk environment was another consideration. As
the amount of efforts and resources increased over time, in particular, expanding beyond basic policy mandates, business and senior managers would begin to question the cost of security. Should business systems or any information assets be subjected to new attacks that have not been addressed by existing policies, information security risk managers would be caught off-guard, and business management would also penalize them for the security breaches. As such, there have been pressing needs for information security risk managers to find new ways to justify the value of information security, and the investment required, beyond the reason of compliance with policies or regulations.

2.5.4 Communication

The need for communicating information security have been motivated by the common belief that “many instances of data loss/corruption or computer service unavailability can be avoided if personnel are properly trained” (Dorey, 1994, p. 53). There have been numerous studies focusing on the execution of this aspect of the information security program. For example, Kovacich (2003), Siponen (2000a), and Yngstrom’s (1995) studies on the planning and delivery of security awareness and education programs, respectively. Hinson (2005) also provided an informative summary on the value of information security awareness. Research institutions such as the Center for Information Systems Security Studies and Research (CISR) have also undertaken various studies relating to peoples’ security competency, in particular, on education and curriculum for students new to the field.

The need for a security program to incorporate training to build up people’s psychological awareness and resistance against social engineering attacks, such as requiring individuals to challenge strangers and improve understanding of individuals’ security responsibilities were also recognized early in the development of the information security field—for examples, see Dorey (1994, pp. 53-56), Mitnick (2002), and Siponen (2000a; 2000b). While studies and suggestions have been available from a social psychological perspective—for example, Kabay (1993; 2002)—for improving security awareness and practices, social engineering risk has remained as one of the highest on the Internet. In a study on the interrelationship and effect of culture and risk communication on setting Internet security goals, Koskosa and Paul (2004) concluded that “these perspectives have an ultimate effect on the
level of security goal setting”. Studies on the social-technical aspects of information security risk management in organizations are therefore needed to further understand the issues and dilemmas in practice, and to find new strategies, approaches, and/or models to improve the situation.

2.5.5 Developments

Identifying security requirements and incorporating them into the design and development of IT systems, applications and products in organizations, as part of the systems development life cycle, has been critical to the success of information security. They have affected not only the security outcome of the organization’s information assets, which involved information system, applications, and products, but also the follow-on operational security and supports. As discussed in Section 2.5.6, poorly designed applications or systems would lead to difficulties in administration, monitoring, and enforcement of security policies.

In this regard, Baskerville (1993) has taken a social perspective in studying the security considerations for designing and developing information systems products and applications. Howard and Lipner (2005), Howard and LeBlanc (2003) and others have also extensively studied the engineering aspects of designing and developing in software information security requirements, and implementing them as part of organizational “Security Development Lifecycle” practices. A formal standard with respect to this aspect of information security was also published by the U.S. National Institute of Standards and Technology (NIST) in June 2004, providing guidance to U.S. federal departments on the security considerations to be made in the information system development life cycle (Grance, Hash, & Stevens, 2004).

Howard and Lipner’s inclusion of a response element into their security development life cycle signified its consideration for changes and updates required, which differentiated it from the other approaches. The question of how a security development life cycle should support a rapidly changing risk environment however has remained relatively new in the field.

2.5.6 Operational Security

The term “operational security” has been used quite differently in two different contexts. In the military, it referred to securing the environment and systems in an
operational environment, for example, in a training area or a battlefield. In business organizations, it normally referred to operating the security functions as part of the IT operation management efforts. In this regard, it has included security administration, security monitoring, incident response and handling, and business continuity and recovery.

In most organizations, using the “Protect-Detect-React” (PDR) strategy, which was biased towards the use of controls for risk mitigation, most emphasis has been placed on administration, which included selecting appropriate controls as protective safeguards, installing and configuring those controls, maintaining configurations, and administering users’ use of the systems and related controls (for example, user identifier and password maintenance, user identifier re-certification, and maintenance of access control listings on information resources in systems). Referring to the problems of security administration, Dorey emphasized that a large part of “mal-administration” processes, including installation, configuration, maintenance, and monitoring, are related to the design of the application, product, or systems catering to the business needs and security requirements. Security requirement considerations, including operational security considerations, were therefore critical to operational security. In addition, the technical expertise of the security staff, including their understanding of security policies and requirements and ability to map both together to determine suitable configurations and parameters for monitoring and enforcement in different use scenarios were also crucial (Dorey, 1994, pp. 61-66).

While more automation and integration of security management requirements into technical systems and solutions (as suggested by Dorey and others) would reduce the “mal-administration” issues, it was also important to understand the social behavior and related changes in relation to the changing risk environment, and when different security strategies were undertaken (instead of the PDR strategy). Understanding the social practices and related issues in current practices in the operational security areas of the information security program, and the potential impact (positively or negatively) on the security administration and management processes (relating to people, in particular) in relation to a change of security strategy were therefore of particular interest in this study.

Besides administration and management, operational security has included planning and executing incident response, handling, and management, and business continuity
and disaster recovery planning. Although these have also been recognized as critical areas in information security risk management, studies and literature in these two areas were mostly vertically (silo) oriented, focusing in the area of damage control, and recovery, for example, see Greenberg (2003, p. 63).

In business continuity and disaster recovery planning, they were considered as separate functions from the information security function in organizations, for example, see Dorey (1994, pp. 36-37), even though they were increasingly regarded as essential elements of an information security management system (ISO/IEC, 2000, 2005e). Consequently, planning and execution of business continuity and disaster recovery were often undertaken by different individuals in the organization.

### 2.5.7 Performance Measurements

In the United States, a number of new regulations have included IT security performance measurement as a requirement. The U.S. National Institute of Standards and Technology (NIST) has since also issued guidance on “how an organization, through the use of metrics, [can identify] the adequacy of in-place security controls, policies, and procedures” (Swanson, Bartol, Sabato, Hash, & Graffo, 2003). The NIST standard (SP 800-55) aimed to

provide an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments (Swanson et al., 2003).

Such metrics were however focused on measuring the effectiveness of security controls implemented, but not how well an Information Risk Manager has performed his/her job in the risk assessment, security controls design and selection, or implementation.

Recently updated security standards such as the ISO/IEC 27001 (2005f) have also emphasized the need and importance of performance and effectiveness in the information security management system requirements that they promulgate. New standards specific for measuring the performance of information security management system, in relation to the implementation of ISO/IEC 27001, has also started development in the ISO/IEC JTC 1 SC 27 working group. NIST (Chew, Clay, Hash, Bartol, & Brown, 2006) has also produced a new guidance on performance metrics.
for information security (SP 800-80), complementing the earlier guidance (SP 800-55).

The various standards and guidance have proposed a programmatic approach for aligning performance measurements to the objectives of information security in organizations.

One of the common measurements for the effectiveness of information security was the state of security delivered by the information security program. Maiwald and Sieglein (2002, pp. 180-188) discussed two methods of reporting – metrics and risk. Metrics was related to reporting measurable security attributes such as the number of system vulnerabilities, number of policy configuration violations, number of detected attacks on network, number of employees reached by a security awareness program, number of failed access attempts, and number of security incidents. These attributes would essentially reflect the stability of the risk environment. Risk was related to the progress of the risk reduction activities, as part of the information security risk management program, since the successful completion of such activities would result in eliminating or reducing the related risk.

The usefulness of Maiwald and Sieglein’s proposed metrics was however limited.

In organizations where preventive security controls have been implemented, the organization might enjoy a period of stability (i.e., zero or few security incidents), until a security exposure has been discovered or an incident occurred. Note that the specific length of this period would be uncertain. No incident has different meaning than security as well. It might be that the perpetrator has not yet identified the organization as a viable target, or a potential perpetrator has not found a meaningful use for the known exposures or vulnerabilities in the organization at a given point in time. Hence, they have not been exploited. Similarly, a perpetrator might have already been using identified exposures to conduct subtle reconnaissance to plan for something bigger, which would remain covert until the incident has emerged. There were potentially many possibilities. Using stability (by counting the number of incidents, vulnerabilities, or violations) as a measurement was therefore inadequate to determine the security status of the organization.

A more detrimental side effect of using stability as a measurement would result when if the senior management developed a false sense of comfort from the lack of incident
and perceived no necessity for new investment in security protection. Nonetheless, when a security incident occurred due to an attack on a newly-discovered security vulnerability, losses or damages would be incurred. Given that there was a security incident, the effectiveness of the risk manager, cost of security and its return on investment would also become questionable, even though its significance depends on the context and seriousness of the actual incident. An incident with significant damages might also cost the information risk manager’s job.

Clearly, if known risks and attacks continued to result in negative impacts on the organization, the risk manager’s approaches and measures would be questionable. The risk manager would need to re-evaluate and change her/his strategy and tactics in order to address the problem. Having a large number of security incidents on known risk issues was unacceptable despite not being an adequate indicator for the organization. However, neither would few (or zero) incidents mean a well-protected organization. Security incidents and the security status of an organization therefore have a non-linear relationship. It was therefore necessary to also consider other attributes of the associated events when incorporating them in performance measurement.

In addition to the use of metrics and risk, Maiwald and Sieglein have suggested tracking the return on security investment (ROSI) in terms of how security provisions in business projects have enabled business opportunities and/or resulted in cost savings, for example, lower company insurance premiums due to better security (Maiwald & Sieglein, 2002, p. 188). The use of economic models, such as ROSI, to evaluate security investments have in recent years garnered substantial interest in the research arena, and numerous models and approaches have been published, for example, Gordon and Loeb (2002), Mercuri (2003), and Rodewald (2005). For a comprehensive list, see Anderson (2006).

Cavusoglu, Mishra, and Raghunathan observed that the lack of a comprehensive model that incorporates the specific features of IT security technologies has prevented firms from applying rigorous quantitative techniques to make security investment decisions. The current set of tools such as risk analysis and cost effectiveness analysis work with very high-level aggregate data, so these tools are of limited value in an IT security setting (Cavusoglu, Mishra, & Raghunathan, 2004).
Cavusoglu, et al. proposed a probability model to evaluate IT security investment based on the potential damage that could result from the impact of a risk realization. A risk assessment was a pre-requisite to the use of this model. The value of alternative IT security investments, for example, to set up a perimeter network infrastructure against the risk of potential hacking attacks on the company network versus acquiring such a network infrastructure from a third party network provider, was analyzed against the potential damages to determine the “best” approach, based on the maximum cost savings between the alternatives.

One challenge in such an approach (and also in other cost-based analyses of security investment) was that it relied heavily on past incident data, and predicted that similar incidents would happen. The assumption of similar incident occurring covered only a limited scope of potential risk of the organization, and have not adequately accounted for uncertainties. As highlighted in Section 2.3.6.2, there were limitations in both probability and statistical measurements, which therefore made such techniques subjective.

The cost savings could be misleading, since it was not always possible to establish a clear relationship between any past incidents that have not recurred and the work of the security investment. More importantly, future incidents would likely be different, in terms of the way the hackers might attack a system, the existence and forms of vulnerabilities that might be exploited, the potential impact, and the scale involved. The capability provided by the security investment in protecting against new instances of attacks would be an obvious benefit to a company. However, if the security investment was focused only on addressing past issues, it would be unlikely to withstand future attacks that have employed different tactics, or have exploited new vulnerabilities in the system. If the investment was to address new attacks, it would face the challenge of predicting the tactics and nature of attacks, including their possibilities and potential impact, since no data about future attacks would be available in the first place.

The possible use of such an approach was then limited to justifying spending (or investing) against known (identifiable) risks, in particular, pervasive risks that would recur easily when not protected against.
Citing Marin (1992), Bjorck asserted that “the optimum level of security, from a strict financial perspective, will be found in the situation in which the cost of additional security countermeasures exactly equals the resulting reduction in damages arising from security breaches”, which meant “profit maximization” for the organization (Bjorck, 2005, p. 27). However, citing Adams (1995), Bjorck (2005, p. 28) also reported that:

in many cases, the total cost of current security countermeasures and the damages arising from current security breaches are not known. And, looking into the future, the potential costs-and-benefits of new countermeasures are even more challenging to estimate.

From a regulatory perspective, with an increased emphasis on management accountability, senior management could potentially face the “risk of incarceration” if they focused their efforts too much on return on investment (Berghel, 2005).

Another approach adopted by some organizations to determine their security status was to conduct benchmarking of the company’s security practice, incident count, financial and/or reputation impacts from actual incidents, audit ratings, and a series of other measures compared to those of other organizations in the same industry. Such an approach has several limitations. The timeliness of information and response, the company’s organizational and risk culture, and the business operations practices often differed even among companies in the same industry. An alternative approach suggested in Bjorck (2005, p. 57) was to perform an “evaluation benchmark” against a specific standards such as the ISO/IEC (2005e) 17799, and ISO/IEC (2005f) 27001 ISMS. While standards were comprehensive in their scope of coverage, their use should be based on risk assessment of the organizational information risks and requirements.

As such, in either case, benchmarking could only provide an indication of the maturity of the organization’s information security practices compared with its peers or a selected standard, but not reflecting the risks and uncertainties that it was facing in information risk management. From a budgetary standpoint, its usefulness was also limited (J. Jones, 2007).

The challenges of current approaches for performance measurement confirmed the need to address the third question relating to the thematic concerns of this study:
Chapter 2 – Literature Review

How should organizations resolve the conflict between the performance measurements of the information risk manager and the outcome of a security incident? Should the information risk manager’s performance reflect the security risk status of the organization, or, in other words, what should the relationship be between his/her performance and the security status of the organization (Section 1.3)?

While measuring performance and effectiveness of security (be it in terms of investment or resources used) was critical from a management perspective, what have been measurable, however, were past events and status data, which would only provide an indication of the likelihood of the organization to survive in the known risk environment. To understand its true performance in terms of its status of security, organizations need to move from understanding the past to the present. What should be monitored and measured in order to understand its present risk status, and a means of translating the measurement to the capability of the organization to deal with changes in the risk environment were, however, lacking in existing literature. This was another issue requiring further studies, which supported the second research question:

How should Information Risk Managers manage the information security risk in a constantly changing business and IT risk environment, such as (1) security risk development in the information technology arena that could disrupt the business and/or IT operations, and (2) changes in the business and/or IT strategy and implementation that could significantly change the organization’s risk posture? (Section 1.3)

2.6 Responding to Change

As observed from the literature review covering the scope of information security risk management discussed in the previous sections, one of the main recurring themes in current studies was the issue of dealing with changes in the risk environment. The review showed that responding to change has become a key attribute in ensuring effective information security risk management. This was also reflected from the works of Anderson (2001b), Yourdon (2002), and Gupta, Chaturvedi, Mehta, and Valeri (2002) summarized below, in which they have studied the problems of information security management from different perspectives.

From a macro economic perspective, Anderson observed that “information insecurity is at least as much due to perverse incentives”. The effects of “network externalities”
were that commercial systems will often have a tendency to delay new features (including security features) to the next version, for reasons of economics. As such, changes in technology systems were persistent. Similarly, for competitive reasons, “constant struggles to entrench or undermine monopolies and to segment and control markets” would also continue, further affecting many of the environmental conditions in which security systems have to keep up to date and address related risk. Over time, due to market pressure, security technology and IT systems in general would improve in their resiliency and reliability. They, however, would not get to a point that will provide 100%, or near 100%, security (Anderson, 2001b). This was also suggested in the “no perfect security” principle discussed earlier in section 2.3.5.

From the perspective of information warfare, the technical bias further favored the attackers rather than the defenders, since the defender has a much larger surface area to protect, whereas the attackers would just need to look for a single weak link to strike. This has been worsened by the theory of asymmetrical information, which has encouraged potential attackers as finders of security vulnerabilities to keep the vulnerabilities that they have found to themselves for use in later attack operations or simply to sell them for a profit (Grow, Hamm, Greene, & Lacy, 2005), instead of reporting them to the vendor, which would help to protect the defenders and make the job of the attackers harder.

The macro economic analysis showed that “the management of information security is a very much deeper and more political problem than is usually realized; solutions are likely to be subtle and partial, while many simplistic technical approaches are bound to fail” (Anderson, 2001b).

In analyzing the security implications following the September 11th, 2001 incident (Kean et al., 2004), Yourdon identified the need for a paradigm shift in risk management, and emphasized that:

[T]oday’s risks can occur and then change so quickly, and because they may involve completely unfamiliar situations, the “official” information about risk-status and risk-mitigation may be obsolete, misleading, ambiguous, or downright wrong. When given information about potentially serious risks, it’s extremely important to look for alternate, independent sources of information—e.g., from news media in other countries—before reaching a conclusion about what to do (Yourdan, 2002, p. 154).
In Gupta, Chaturvedi, et al. (2002), their experimental analysis of the implications of security policies and risk management approaches in online banking systems established that being “proactive in recognizing the threats and devising policies to counter them generated greater revenue and were able to focus on the core activities”.

From a management strategy perspective, Gagliardi commented that:

> We must also understand that no position is perfect for meeting every challenge, and there is no position that does not degrade over time. There is no ultimate victory that ends the strategic struggle. There is no final resting place where everything is perfect. No matter how far we advance, we will always be confronted with new challenges (Gagliardi, 2004, p. 19).

In numerous studies that called for a change of paradigm, or for new strategies or approaches to be devised to address the issues and dilemmas of information security risk management, for examples, Hoo (2000), Dhillon and Backhouse (2000; 2001), Blakley, McDermott, et al (2001), Yourdon (2002) and Bjorck (2005), none have been specific about how to respond to change when managing information risks in organizations. As far as change was concerned, current literature have focused mainly on the changes relating to Internet proliferation, and how to address the information security issues resulting from those changes. Dealing with change, or, managing change, has been regarded as one of the major issues in current paradigms, strategies, and approaches. In the practice environment, change has also been recognized as a significant contributor to IT failures in organization (Mayengbam, 2006).

### 2.7 Current Research and Social Perspectives of Information Security

In recent years, more studies have been undertaken in the combined topic of information security and risk management, in particular, focusing on two aspects: (1) the economics of information security (Anderson, 2001b; Anderson & Moore, 2006, 2007; Gordon & Loeb, 2002), contributing to the quantitative measurements of information risks and related investments; and (2) social aspects of information security management, to gain better understanding of information security risk management practices in organizations, including the design and implementation of security management programs, awareness, education, and training (Clarke & Drake, 2003; Dhillon & Backhouse, 2001).
The interest in the economics of information security risks was assessed to be a response to achieve a greater understanding of information security in relation to business risk, and the cost and investment that business management have been focusing upon when deciding on security spending. The interest in the social aspects of information security was assessed to be motivated by the recognition of the fact that people has often been the weakest link in a security chain. In studying the technical aspects, including the economics of information security, there was also a need to regard the social implications, and leverage the psychological and social characteristics of human and group behaviors to make advancement in information security.

In studies conducted by Clarke and Drake (2003), and Dhillon and Backhouse (2001), which both adopted the sociological paradigms presented by Burrell and Morgan (1979), they found that most research and literature relating to information security were predominantly technical and functionalist preconceptions. They were largely rule-based and control-oriented when devising strategy and solutions to information security problems. Dhillon and Backhouse attributed this to the methods used, which have mostly been “grounded in a particular well-defined reality, i.e., that of the military”. This, however, was not the only issue. As discussed in the beginning of Section 2.2, researchers have the tendency to take a reductionist approach to information security problems. As such, most studies tended to focus on the data instead of the information, and technology instead of systems.

Clark and Drake observed that there were “poor theoretical grounding for information security as a discipline, and literature which is available casts the field as one focusing on secrecy and restriction, in which a rule-based approach is seen to be relevant”. As reported by Kang (2004), Clark and Drake’s claim that current research were focused mainly on secrecy (or confidentiality) was however “not accurate”. Citing Clark and Wilson (1987) as example, Kang asserted that “the sequence of information flow and information integrity and availability were being studied and emphasized as early as the 1980s”. As also highlighted earlier in Section 2.2, Kang added that “Parker (1998) have suggested several limitations [relating to the use] of the [Confidentiality, Integrity, and Availability] model, and proposed including usability, authenticity, and possession”. 
These are also generally recognized as implicit characteristics to availability, integrity, and confidentiality. It may be worth considering these other views from the critical theory perspective and participants’ views before concluding that current emphasis has been on confidentiality (Kang, 2004).

In addition, when applying the sociological paradigms to analyze information security studies and literature,

…the context of use and security requirements should be considered. If a different security requirement is desirable or inherent in a specific view, then perhaps we should consider taking a different view when the context differs (Kang, 2004).

In any case, the review conducted in this chapter showed that discourses on the different approaches and methods have not been profound, especially in the sociological context and perspective.

Clarke and Drake also reported that a trend towards the interpretive paradigm has become obvious. However, “social theory suggests problems with interpretivism, in that the kind of open debate necessary for human viewpoints to be recognized and acted upon may be suppressed or distorted by power structures within a social, and particularly organizational, context” (Clarke & Drake, 2003). Such a phenomenon may also be attributed to the lack of a professional standing of the information security risk management profession, a topic that has gained concerns and attention in the recent years (Piper, 2006).

According to Dhillon and Backhouse, their “literature search found few examples of a social-organizational perspective for evaluating information systems security, pointing to a greater need for more empirical research to develop key principles for the prevention of negative events and therefore to help in the management of security”. Similarly, in a study on information security management, Bjorek (2005, p. 142) reported that “empirical research on the management of information security is [still] lacking”.

With direct participation in the social context, this study is therefore an important undertaking that also contributes to the social-organizational perspective of information security risk management.
2.8 Conclusion

While the weakest link principle promotes the adoption of a defense in depth strategy for information security, defense in depth creates complexity and adds cost to the business. Complexity results in emergent behaviors, which can be adverse, and create new weak links in the system. Increasing cost drives the reduction of security measures, therefore removing layers of defense or protection, and bringing in opportunity for weak links to exist. Focusing on removing the weakest link and the application of defense in depth, which keeps removing the next weakest link is like attempting to achieve perfect security, which is known to be overly costly and an impossible outcome.

Risk management appears to be a solution that strikes a balance between defense in depth and the drive for security perfection. Applying risk management, however, issues that are assessed as low risk will normally be accepted without mitigation. Retaining or accepting risk means leaving gaps in the system. This may end up as weak links waiting for perpetrators to exploit.

In addition, the outcomes of risk analysis and assessment are also subjective to the knowledge and experience of the analysts. When an analyst assesses an issue as having a potentially low risk to the business, due to lack of historical data, and little to no knowledge of the risk relating to the future, it is a subjective assessment. There is therefore a chance that a low risk item may actually become high risk when the systems environment changes and evolves.

The notion of risk compensation, as highlighted in Adam (1995), has also shown that risk cannot be completely managed. The moment we attempt to deal with a risk, the risk itself will change. As such, there is always an element of uncertainty. In current information security practices, as personally experienced in the practice environment, the notion of risk compensation and the element of uncertainty have either been ignored or ill considered. There has also been a lack of suggestion on how to deal with such phenomenon even when one is to consider them. To be effective, information risk managers have to consider such risk phenomenon and address them as part of the risk management strategy and plan. Most organizations rely on an incident management and recovery plan, which deals with the aftermath of incidents, but not when changes to the risk environment have been detected.
In summary, while the underlying principles of information security are individually sound, they do not necessarily complement each other and resolve the primary issue of weak links. Alas, they cause conflicts, resulting in a circular problem. How should information risk managers respond? This, inferring from the review and synthesis of current literatures, raises the question of whether current approaches of using traditional risk management strategies and techniques to achieve information security are indeed adequate or practical. The question suggests the need for more studies and research in the practice of information security risk management.

In the above review, it is also clear that current literature and researches on information security risk management have continued to place significant emphasis on the technical engineering aspects to improve or renew the tasks, technology, and processes involved in managing information risk resulting from the convergence and proliferation of information technology and systems in the new millennium.

Recognizing the critical role that people play in organizational systems in managing information risk, since the late 1980s and early 1990s, studies on managing information security have begun to shift towards understanding the social phenomenon relating to this field. However, focus has remained on specific sub-domain of the field, such as system design and development, and security awareness and education, but rarely at the strategic management level.

Since early 2000, researchers have also been looking into the economics of information security to better understand the issues and dilemmas of managing information risks. In their attempts to quantify risk and security investments to better justify for the needs, technology, and processes of information security risk management, it has become clear that the problem of managing information risk is hard because of the constantly changing nature of the problem space. Changes are inherent not only because of business changes or technology development and proliferation, but more subtly, reasons of market economy, and political and competitive advantages to be gained by various stakeholders and the supply-demand chain of business.

These outcomes indicate the need to focus on responding to change for managing information risk, which is largely missing from the literature.
Analyzing and interpreting the synthesis of the literature reviews, I inferred the following propositions:

1. Information security risk management should be responsive to change, or capable of dealing with constant change in the information risk environment.

2. Information security risk management problems, though considered “hard” (as in difficult and complex,) in the grammatical expression as suggested by Anderson (2001b), are not exactly hard problems from a research perspective. Instead, information security risk management systems are essentially part of a Human Activities Systems (HAS), and therefore a class of “soft” problems, as suggested by Checkland (1999), Checkland and Scholes (1990), and Checkland and Holwell (1998).

3. To understand the phenomenon of information security risk management, and improve the practices in the field, studies should evaluate the social (i.e., “soft”) human behavioral aspects of managing information risks, in particular, in the practice environment where the actual technology, processes, and people interact and deal with information risks.

4. Besides focusing on the social aspects of information security risk management, researchers must not lose track of two other critical aspects of information risks that have been part of the technical research paradigm:
   a. The close relationship between information risks and information technology; and
   b. The constantly changing nature of the technology, business systems, and environment.

5. The two aspects—social and technical—are co-producers of the intended outcome of information security risk management. The distinctive characteristic of each must be respected, or else their contradictions will intrude and their complementarities will remain unrealized.

The above propositions suggest the need for a “paradigm shift”, that a study taking a social-technical approach to information security risk management, encompassing both the social (“soft”) and technical (“hard”) aspects of managing information risks, and taking into consideration the need to deal with, or respond to constant change in
Chapter 2 – Literature Review

the information risk environment, is critical for gaining better understanding and improvement of the practices.

The approach should provide further understanding, and help find suitable answers to the following research questions that were identified in the practice environment summarized in Chapter 1:

1. What should an Information Risk Manager do differently or change in his/her strategy and plan in managing information security risk for the organization in order not to have them result in a compliance driven, and/or control-oriented security culture to be able to deal with the security challenges in a constantly evolving and changing business and IT environment?

2. How should Information Risk Managers deal with the ongoing information security challenges faced by their organization due to both external and internal changes in the business environment?

3. How should organizations resolve the conflict between the performance measurements of the information risk manager and the outcome of a security incident? Should the information risk manager’s performance reflect the security risk status of the organization, or, in other words, what should be the relationship between her performance and the security status of the organization?

Chapter 3 describes the selection and justification of research methodology for studying the above propositions and questions, in the practice environment described in Chapter 1.
3 Research Methodology

3.1 Introduction

In Chapter 2, we concluded that in pursuit of better understanding and improvement in information security risk management in organizations, studies using a social-technical approach will be of significant value to the field. In addition, the research questions identified in Chapter 1 and re-affirmed through the literature review in Chapter 2 both pointed towards the need for new approaches to focus on responding to change in the risk environment. These criteria formed one of the bases for the selection of the research methodology in this study.

To ensure the soundness, validity, and rigor in the research outcome, within the bounds of ethical considerations, quality criteria are also needed to be identified. The criteria influence the selection of the methodology and the conduct of the research, including procedures for data collection, analysis, and interpretation.

Action research, an iterative research methodology that has been commonly used for studying social changes, and also successfully applied in management and organizational problems and situations that were technical in nature—for examples, Chee (1999), Goh (1999), Kwok (2001), Sankaran and Sng (2001), and Tay (2003)—was selected as the research methodology for this study.

This chapter provides justifications for the selection and use of action research as the research methodology, including identification and discussion of the quality criteria and the research procedures employed for data collection, analysis, and interpretation throughout the study.

3.2 Justification for using Action Research

Research is a broad topic. There are, however, many types of research, and numerous views as to the nature of each, what it aims to achieve, and how it should be conducted (Costello, 2003). Before the actual conduct of a study, these aspects of the research need to be clarified. As highlighted in Gregory (2003):

We expect anything that passes as research to have a certain integrity… What is intolerable in respect of research is the deliberate disregard of the canons governing the conduct of research. Research is driven by the desire to advance knowledge and
understanding (on our own part, and, if we are lucky, on behalf of others). The very purpose of research, at the more mundane as well as the loftier levels of research activity, can only be served by taking seriously certain intellectual demands intrinsic to the advancement of knowledge and understanding (Gregory, 2003, p. 14).

We shall therefore examine the criteria essential to the conduct and outcome of research before justifying the selection and use of action research as the meta-methodology or research paradigm for this study.

### 3.2.1 Criteria

Traditionally, research methodologies have been classified as quantitative versus qualitative (Gill & Johnson, 2002), and the design of a specific study may be characterized as fixed or flexible (Robson, 2002). While fixed design research is mostly quantitative and experimental, and flexible design research is mostly qualitative and interpretive, the design itself does not preclude the use of either a quantitative or qualitative research methodology.

Quantitative research used to be regarded as the only “scientific” method for conventional research, and is common in experimental research, in which the research is often conducted in a laboratory, or a near-laboratory condition environment, producing quantitative results, usually in the form of statistics to support a hypothesis.

Qualitative research methodologies, such as ethnography (Gill & Johnson, 2002, pp. 10-11, 165-167; Myers, 1997; Robson, 2002, pp. 186-190), are at the opposite end of the spectrum. Qualitative researchers aim to induce knowledge through an approach that emphasizes the analysis of subjective accounts that are generated by being part of the situation and involve the investigator in the everyday flow of life. Emphasis is on theory grounded in empirical observations which take into account the subjects’ meaning and interpretational systems in order to explain the understanding learned from the study. This approach generates and uses mainly qualitative data and minimum structure.

Quality is one of the most important criteria in research (Trochim, 2000). The concepts of validity and reliability are often regarded as fundamental to the quality of research (Gill & Johnson, 2002, pp. 162-191; Hoover & Donovan, 2004). Adding “generalizability”, Robson (2002, p. 93) summarized these criteria as important for determining the “trustworthiness” of research.
According to Gill and Johnson (2002, pp. 162-163), validity refers to the approximate truth of propositions, inferences, or conclusions. Validity has included internal, external, and construct validity. Internal validity determines whether or not “what is identified as the ‘causes’ or ‘stimuli’ actually produce what have been interpreted as the ‘effects’ or ‘responses’”. “External validity” refers to the extent to which any research findings can be generalized or extrapolated beyond the immediate research sample or setting. “Construct validity” refers to the degree to which inferences can legitimately be made from the operations in the study to the theoretical constructs on which those operations were based. Like external validity, construct validity is related to generalizing, but where external validity involves generalizing from the study context to other people, places or times, construct validity involves generalizing from the program or measurements to the concept of the program or measurements.

Gill and Johnson (2002) have further subdivided external validity into “population validity” and “ecological validity”. Population validity refers to the possibility to generalize from the sample of people involved in the research study to a wider population from which the sample was drawn—an important measure in quantitative studies. Ecological validity, which applies more directly to qualitative studies, refers to the possibility to generalize from the actual social context in which the research has taken place and data thereby gathered, to other contexts.

“Reliability” refers to the consistency of results obtained in research. In the context of quantitative research, reliability means that “the measurement(s) of variations can be replicated by others” (Hoover & Donovan, 2004, p. 52).

As highlighted in Robson (2002), most of these validity and reliability criteria “were initially developed in the context of traditional fixed designs collecting quantitative data, and there is considerable debate about their applicability for flexible designs with qualitative data”. As such, alternative criteria have been proposed by other qualitative researchers. For example, Greenwood and Levin (1998, pp. 80-85) suggested credibility as another concept for assessing the quality of social research. “Credibility” is defined as “the arguments and the processes necessary for having someone trust [the] research results”.60

A serious side effect of using alternative quality criteria for qualitative research is that they end up “providing support for the view that qualitative studies are unreliable and
invalid” (Robson, 2002, p. 170). Zuber-Skerritt (2001, p. 5) asserted that the meaning of validity and reliability should vary between research paradigms. Citing Reason & Rowan (1981, p. 244), Zuber-Skerritt highlighted that “validity in the new [phenomenological, interpretive, and mainly qualitative] paradigm is more personal and interpersonal than methodological, and should be based on an interactive dialectic logic rather than a dichotomy of ‘subjective’ or ‘objective’ truth”.

This dichotomy can be overcome by the concept of “perspective”, i.e., taking a personal view from some distance and after an interactive dialectic using multiple data, respondents, and co-inquirers (Zuber-Skerritt, 2001, p. 5).

Supporting the relevance of the validity and reliability criteria, Dick suggested that:

What we know or think that we know of [some part of the world] may be a mental construction -- and I assume it is. I assume also that our mental construction stands in some relationship to the world “out there” that exists as real or actual, rather than simply as a mental construct. And it is “out there”, a palpably real or actual world, that we wish to influence.

On the grounds explored above, it seems to me that reliability and validity are still useful concepts. For example, it is still my intention that as far as possible the information I collect is not idiosyncratic; that it is to some extent reliable. I attempt also to discover as accurately as I can the experience that my informant describes so it is to some extent valid. The greater the validity and reliability of the information and insight that I obtain, the greater my confidence when I draw on my understanding to take action (Dick, 2000d, 2002e, p. 166).

It is therefore clear that there is value of using common yardsticks such as validity and reliability as quality criteria in research. In addition, there are procedures that may be adopted to verify the outcomes of the study and ensure validity, for example, see Glesne (1999, pp. 32-33) and Robson (2002, pp. 172-176).

In terms of reliability, for qualitative researchers, thinking in terms of using standardized research instruments, formal tests and scales to achieve consistency of results is problematic. Instead, they have to “concern themselves seriously with the reliability of their methods and research practices”, and be very “careful and honest in carrying out their research”, with the use of tools such as an audit trail to provide documented evidence of their investigations (Robson, 2002, p. 176).
On generalizability of the research outcome, while it may appear to be a difficult issue, Dick (2000d) commented that most “qualitative researchers have given up too easily”. There are some trade-offs between discovering general truth and results being relevant to local situation. Generalizability of the results in action research may be developed through logical analysis, multiple case studies, use of higher diverse samples, and/or comparison of the interpretation to those in the relevant literature (Dick, 2000d). Fixed-design experimental setting of quantitative research may produce a specific outcome in the laboratory. However, the outcome will often rely on a set of stated assumptions and variables. When the results are brought to a practice environment, or operationalized, the earlier assumptions may not necessarily persist, and other variables may also emerge. These affect the actual outcome and may invalidate the research findings before generalization of the research outcome can actually take place. As also noted in Zuber-Skerritt (2001, p. 7), “generalizations might be statistically purposeful and significant, but they often are not applicable or [are] irrelevant to the individual case and specific group”.

In qualitative research such as case study research (Robson, 2002, pp. 177-185) and action research (Dick, 2000d, 2001), the practice environment is the “laboratory”. The research data are the real world data. Given the relatively natural, non-artificial settings, such research methods are seen to “gain naturalism and therefore are relatively higher in ecological validity” (Gill & Johnson, 2002, p. 164). The research outcome can therefore be used as a new starting point for further studies in a subsequent environment.

Kathryn Herr and Gary Anderson (2005, pp. 61-64) described this as the concept of “naturalistic generalization”, and the notion of “transferability”, citing Robert Stake (1986) and Lincoln and Guba (1985), respectively. Since the original inquirer cannot know the sites or situations to which the new found knowledge and theory might be applied or transferred, the applicability or generalizability of the knowledge lies more with the person seeking to apply it, rather than the original researcher who discovered it. Dick (personal communication, June 12, 2006) added that “the researcher can also aid generalizability by describing the situation carefully and by defining the boundary within which the research results can be assumed to apply”. As such, if the knowledge can be applied in a new context, or proved applicable through matching the similarities of the problem situation and the environment, knowledge has been
transferred, hence generalized. Using action research, the outcome of each action research cycle is applied to the next and the possibility for subsequent cycles to produce evolved outcome. It therefore supports the notion of naturalistic generalization, or transferability.

### 3.2.2 Methodologies and Meta-methodology

Besides the criteria for determining the quality of research, there are also inherent strengths and weaknesses in the respective methodologies that should be considered in research design and structure.

#### 3.2.2.1 Quantitative, experimental, and positivist

The need to have a hypothesis, to set up a suitable environment as the laboratory for the research to develop suitable metrics (or variables) and tools for measurement, and to focus on quantitative data and results in the design and structure of experimental research have brought substantial progress in the world of natural and physical sciences. Those advances have substantiated quantitative research with significant strengths of internal validity and reliability. However, such an approach, commonly known as the “positivist paradigm”, for example, as seen in Zuber-Skerritt (2001), has limitations when we try to apply it to management research, given its low naturalism, i.e., low ecological validity, as described in Gill and Johnson (2002). Such limitations restrict its use in the non-laboratory environment—in real world organizational settings where all things (people, process, and technologies) are in constant flux both within and outside the organization, and influence each other simultaneously.

To conduct experimental research using quantitative methods requires the environment to behave in a certain manner in order to satisfy the identified assumptions that support the hypothesis. This is not possible in a constantly changing environment, which is where this study has taken place. Change is also a key attribute of the topic involved in this study, as concluded in Chapter 2.

As also noted by Gill and Johnson (2002, pp. 163-164), quantitative research “gains strengths through its high degree of structure, but loses naturalism: experiments are low in ecological validity because of the artificial nature of the research process and [the] context created by their very structure”. Conclusions drawn from quantitative experiments therefore risk being “mere artifacts of the research process and context...
and thus inapplicable to social contexts outside those in which [the] data have been collected”.

When a quantitative method such as a survey involves a small number of subjects, the results of the quantitative study may also lack population validity. However, this may be addressed by “giving greater attention to the random sampling of subjects” (Gill & Johnson, 2002, p. 164).

3.2.2.2 Qualitative and interpretative

While there are critiques of positivism in the quantitative paradigm, qualitative methodologies have their own shortcomings. Their loose structure and highly interpretative approach lend themselves to “subjectivity”, and as such, are often taken to be low in internal validity. However, this depends largely on the rigor of the actual research undertaken, and the context of the problem involved, which can be addressed through specific strategies and procedures relating to the research approach used. For example, see Argris and Schon (1991a), Dick (2001, pp. 24-26), and Glesne (1999, pp. 32-33, 95-112). In addition, as highlighted in Kidder, it is possible to rule out threats of internal validity with the richness of the data and negative case analysis.62

The researcher has many pieces of information about each person or incident… It is this which helps the researcher rule out rival explanations and check hypothesis that are formulated after the fact (Kidder, 1981, pp. 240-241).

This has also been addressed in the methodology selection as described in Section 3.2.3.1.

According to Gill and Johnson, the criticism of the low internal validity of qualitative methodology such as ethnography is “increasingly open to question”, since “ethnographers have a varying commitment to naturalism, they have the scope to rule out some of the threats to internal validity that stem from the artificiality of the research context and procedures; something to which the more structured research styles are evidently victims” (Gill & Johnson, 2002, p. 166).

The reduction in structure may also result in a decline in reliability, as it becomes more difficult for the research to be replicated. We discussed this issue and related focus on reliability required in qualitative research in Section 3.2.1earlier. As also asserted in Kidder,
Chapter 3 – Research Methodology

What matter [in qualitative research] is that each additional piece of evidence is consistent with the other observations and not that each observation is identical…

Reliability in fieldwork lies in an observation’s not being contradicted and proved wrong rather than its being repeated in detail (Kidder, 1981, p. 248).

3.2.2.3 Theory-driven versus data-driven

As highlighted in Hase (2002), “a problem or the research concern is not chosen on the basis of a preferred methodology. Rather, the question is asked and the methodology is chosen later”. Instead of being fixated with a specific methodology and then trying to tilt or mould it to the research issues and scope of study at hand, a different, but pragmatic, perspective, demonstrating the “fitness for the function” may be desired (Swepson, 1995). Dick (2000d) argued that “the most important research choice is not qualitative versus quantitative approach, but that a theory-driven or data-driven approach is a more influential choice”.

Theory-driven research “turns first to a body of extant literature and contributes to knowledge by assuming that literature as a given and extending or refining it, or challenging it”. Most quantitative, experimental, and qualitative, experimental and quasi-experimental methodologies support such a research approach (Dick, 2000d).

In contrast, data-driven research “deals with the research situation and the people in it as they are, as far as possible putting aside [the researcher’s] preconceptions so that [the researcher is] more open to fully experiencing the research situation” (Dick, 2000d). A data driven approach includes methodologies such as grounded theory (Glaser & Strauss, 1999), case study research (Robson, 2002, pp. 177-185), and action research (Costello, 2003; Dick, 1993, 2000d, 2001; Greenwood & Levin, 1998; Kemmis & McTaggart, 1988; Zuber-Skerritt, 2001).

As described in Chapter 1, part of the motivation for this research was to study the practice environment and identify or develop an approach to improve upon the practice of information security risk management within the organization where the study was conducted. A data-driven approach was therefore assessed as an appropriate approach for conducting this study.
3.2.2.4 Meta-methodology

The analysis of methodologies above, and Gill and Johnson’s assertion of the flawed view of treating the use of each as exclusive of the other, in other words, as a “dichotomy”, further suggested “methodological pluralism” as the possibility of “rapprochement between ideographic and nomothetic research methodologies” (Gill & Johnson, 2002, pp. 168-169). From the perspective of being problem-centered, and the learning of complexity theory, Waldrop (1992) and Hase (2002) have also asserted the needs for mixing methodologies.

Given the dynamism of the changing environment and also the context of information security risk management problems, there are opportunities for the use of both quantitative or qualitative methods to obtain data to improve the research rigor, inform the research progress, and eventually produce a better quality outcome. It would be a mistake to prematurely exclude those other sources of data that could potentially improve the validity and hence quality of the research. Methodological pluralism is therefore an important pre-requisite in the research design.

To undertake the research using a data-driven approach supporting methodological pluralism, a methodology capable of supporting, using, and mixing different methodologies based on the data derived from the research situation, and the desired outcome of the next step of the research will be necessary. Tay (2003) referred to this as a “meta-methodology approach”, which has provided an overall framework within which other methodologies may be used, as depicted in Figure 2.

3.2.3 Action Research

The above discourse, evaluated against the context of the research questions and the research environment detailed in the previous two chapters, in essence, have ruled out
the use of a singular positivist, quantitative, experimental approach for this study. The approach to be used will need to support the following:

1. To enable the research to be data-driven;
2. To adopt a meta-methodology, supporting the concept of methodological pluralism, or mixing methodologies; and
3. To enable quality to be evaluated based on the concepts of validity and reliability, applied in accordance with the characteristics of the specific method used at each stage of the research.

Action research (Avison et al., 1999; Costello, 2003; Dick, 1993, 2000d, 2001; Gill & Johnson, 2002, pp. 65-95, 180-189; Greenwood & Levin, 1998; Kemmis & McTaggart, 1988; Pasmore, 2001; Robson, 2002, pp. 215-219; Zuber-Skerritt, 2001) was selected as the meta-methodology, as well as the primary method of inquiry for the undertaking of this study. It was assessed to be a research methodology and paradigm that exhibits the values of both qualitative and quantitative methodologies, in particular, when it relates to the problems to be addressed in this study.

This sub-section argues for the relevance and benefits of action research for use in this study, both as a research methodology and as a meta-methodology. In addition, the limitations of action research and steps taken in the research process to mitigate them are also discussed.

![Action Research Cycle](image)

**Figure 3: The action research cycle alternates action and critical reflection (Dick, 2001)**

Action research, as described in Dick (2001), “pursues both action (change) and research (understanding) outcomes”. The inclusion of action (change) in the research paradigm enables the application of action research to management research in a real live organization directly, as a problem solving process in addition to a research methodology. In its simplest form, as described in Dick (2001), and also shown in Figure 3, the action research method involves two distinctive spirals, or cyclical steps
– action and critical reflection – in which we improve our understanding of the other as the research and actions evolve through the cyclical process.

The two steps may be subdivided further into more distinctive steps, as has been done by many other action research practitioners and researchers. For example, Dick (2001, pp. 24-25) has illustrated that critical reflection may be divided into “critical review” of the previous step, and “planning” for the next step, as shown in Figure 4.

![Figure 4: Critical reflection includes a critical review of the previous step and planning for the next step (Dick, 2001)](image)

The spiral of action cycles may also be undertaken in the following order to increase the researcher’s knowledge of the original question, puzzle, or problem to eventually lead to a resolution:

1. develop a plan of action to improve what is already happening;
2. act to implement the plan;
3. observe the effects of action in the context in which it occurs;
4. reflect on these effects as a basis for further planning, subsequent action and observation, through a succession of cycles (Kemmis & McTaggart, 1988).

More elaborated sub-steps in the action research cycles have also been described in Kemmis and McTaggart (1988), Greenwood and Levin (1998), Robson (2002, pp. 217-219), and Stringer (1999).

### 3.2.3.1 Fitness for the purpose

As highlighted in Dick,

For the research outcome, the most effective research methodology is one that generates information and understanding. For change, you want a methodology which generates commitment to the change (Dick, 2002a).
Action research, which pursues both action and research through a cyclical process, fulfills these needs for effecting change and gaining understanding. As shown in Figure 3, action research cycles alternate between action and critical reflection. Critical reflection can be directed at the data and the interpretations that the researcher is making from it. It can also critique and improve the methodologies that have been used in the study. “Beyond that, it may be used as an opportunity to examine the assumptions about knowledge that inform the research design” (Dick, 2000d).

Our earlier analysis of the quality criteria required for this study (in Section 3.2.1) concluded that a research approach that is qualitative in nature, but at the same time able to provide for the validity and reliability needs, in particular, ecological validity, is fundamental. The tight spiral of action research confers two clear advantages in terms of providing the necessary rigor, which fulfills the validity criteria. (1) Each turn of the spiral provides yet another opportunity to test the interpretation that has been developed against the data collected so far; and (2) Within each turn, a further plan can be developed to put the test in action, and the assumptions that guide the plan. This adds rigor to the research undertaken, and the context of the problem involved, addressing the internal validity issue as discussed in Section 3.2.2.2. As asserted by Dick, “interpretations that survive multiple cycles can be held tentatively, but with some assurance”. The cycle can be repeated (with improvement made based on the earlier outcome) until a final interpretation is reached. Through these cycles, the methodology therefore provides improved quality as desired. By taking steps to ensure that information collected is not idiosyncratic, to some extent, reliability can be attained (Dick, 2000d, 2001).

Prolonged engagement, member checking procedures, peer debriefing, and keeping an audit trail of the research and actions will further support the reliability claim of the research (Glesne, 1999, pp. 32-33; Stringer, 1999, pp. 176-178). Using action research, prolonged engagement will be inherent through the execution of multiple research cycles, which is also necessary to provide rigor. Member checking and peer debriefing can be performed in action research “learning sets”, among peer researchers and/or participants. Journals of action research logs and critical reflections are tools of action researchers, which provide the required audit trails to the research and actions in the study.
Besides considering the merits of action research from the philosophical standpoints (of validity and reliability of the research), it is most crucial that as a research and problem solving paradigm, it must be applicable to the project at hand. In this regard, it must support a data-driven approach, allowing me to deal with the research situation and the people in it as they are, as far as possible putting aside my preconceptions so that I am more open to fully experiencing the research situation as the study progresses.

As highlighted in Dick (2000d), action research, being responsive and flexible, is a suitable choice for undertaking such an approach. However, there are some risks, which are manageable, in the use of data-driven action research. These are discussed in Section 3.2.3.9. More importantly, Dick emphasized two possible outcomes relating to a data-driven action research approach that were relevant to this study, as well as my personal goals:

1. In the course of doing the research, you are able to study and improve your own practice. In effect you use the higher degree as valuable personal and professional development. You may also form a learning set with other postgraduate students for mutual support. Personal and professional development can then be enhanced further.

2. One of the purposes of action research is to improve the research situation. If you research your own practice, it is very likely you will also improve your work situation because you better understand your place in it. The action outcomes you achieve are also likely to benefit your organization or community (Dick, 2000d).

Dick (1999a; 2000d; 2001; 2002a), also cited in Tay (2003), further suggested that “action research can also be used to support a theory-driven process where the goals, plans, actions and methodology can be revised continuously as the research proceeds”. This means that the risk of starting the study with a data-driven approach, which if later found not suitable, can be reduced or addressed when action research is used, is provided that “the goals, plans, actions, and methodology remain within the control of the researcher in the research environment” (Tay, 2003). From a research approach perspective, action research has therefore stood out as a logical choice for the study. This contingency was not however activated throughout this study.
3.2.3.2 Action research as a meta-methodology

The conceptualization of action research as a meta-methodology was introduced in Tay (2003, pp. 60-61), citing Davies (2001, p. 76), who has viewed action research as inherent in humans as an “innate and unconscious process”. As reported in Arnkil (2004, p. 80), other action researchers have also suggested action research as a meta-methodology and good practice.

As a meta-methodology, in each step of the action research cycle, different action and research methods can be adopted or adapted to suit the problem context and execute the actions desired, or interpret the outcomes to gain improved understanding of the process and situations. The specific action and research methods within the action research cycle may be qualitative or quantitative. As a meta-methodology to incorporate, derive or refine other methodologies as mentioned in Hase (2000). Besides Tay (2003), a number of others, like Chee (1999), Goh (1999; 2001), Kwok (2001) and Sankaran and Sng (2001) had also used action research and successfully studied and theorized in their respective problem domain.

As highlighted by Davies (2001, p. 79), action research is particularly useful when the problem or puzzle is “multi-factorial”, which is usually the situation in organizations. Davies, and also Dick (1999a; 2002a) further suggested that action research can start with an ill-defined or fuzzy situation, and then progressively bring focus through the spiral or cyclical process. It does not impose any absolute restrictions on concrete questions. This allows for the “real” issues, and hence thematic questions, to emerge and/or sharpen as the research progresses.

3.2.3.3 Action and change, research and understanding

As discussed in Sections 1.1.1 and 2.6, change is a constant in the business and information security environment, including information security risk management practices. Change may be introduced to evolve a system from no protection to some protection, from some protection to more protection, or adjustment of protection and/or practices to meet new requirements.

Action in the action research methodology stands for change, while research is a quest for understanding (Dick, 2001; 2002a). Action focuses on providing effective change, and therefore a natural selection for planning and taking action to manage change in the field of information security risk management practices. The research component
of action research provides better understanding of the change, from which we can therefore learn from the action, and gain new knowledge in the information security domain.

3.2.3.4 Responsive and flexible

The research questions identified in Chapter 1 and affirmed in Chapter 2 as important issues justifying further studies seek an approach (or approaches) to information security risk management that is responsive to change. In Chapter 2 (Section 2.6), the need for information security risk management to be responsive to change was further identified as a significant gap in the current literature.

According to Dick, action research is responsive to change, and has the flexibility to enable it to adjust to changing needs emerging from the data and situation.

Embedded within an AR [action research] cycle the processes gain the flexibility to be more responsive to the situation. Those conducting the AR can follow the description. They can use the critical reflection within each cycle. Before action they can fit the action to the situation. After action they can check if the action has worked as intended. If not, it can be amended and retried (Dick, 2001, p. 23).

Being flexible and responsive to change, action research therefore can be explored as a potential approach for information security risk management, to determine whether its responsiveness can meet the needs of information security risk management practices. The outcome will provide useful contributions to both the action research and information security risk management knowledge domains, and may henceforth influence future studies and practices in both areas.

3.2.3.5 Process orientation

Information security is a process (Schneier, 2001; 2003). As a meta-methodology (see Section 3.2.3.2) and as a methodology, action research is also process-oriented, and can be adopted to govern the action and research processes, allowing the use of selective methodologies at each stage of the action and research cycle to suit the requirements of those stages. This provides a natural fit between the methodology and the research domain, which should allow for a better understanding of the problem space, issues, and concerns, and through that, identify suitable course of action or approach for resolution.
3.2.3.6 Technical, Practical, and Emancipatory

Action research may be conducted in three ways or progress in three stages along with the learning and experience of the action researcher and participants. These are technical, practical, and emancipatory or critical (Kemmis, 2001; Zuber-Skerritt, 2001). Technical and practical action research can be viewed as developmental processes essential for action researchers before they can fully understand and practice the critical mode of inquiry (Zuber-Skerritt, 2001, p. 9).

In the technical mode, the action research group’s focus is on local problems or issues close to the action researcher, participants, and stakeholders. The participants are viewed as “authentic persons, whose own views were paramount in determining what a ‘problem’ or ‘issues’ or a reasonable interpretation of reality might be” (Kemmis, 2001, p. 100). An outside expert is normally engaged to facilitate, and the relationship between facilitator and participants is mostly co-option, with practitioners depend on the facilitator for actions and understanding (Zuber-Skerritt, 2001, p. 10).

In the practical mode, focus is broadened towards practitioners understanding and transformation of their consciousness. Relationship is escalated towards co-operation, with facilitator encouraging participation and self-reflection.

In the emancipatory stage, the relationship between the participants and facilitator is escalated towards collaboration, with the facilitator as process moderator, and responsibility shared equally by participants. Participants are fully engaged, willing and able to critique openly to bring about transformation of the organization or system. Kemmis reflected that:

In the third stage, the critique of the social macro subject began to have real force in my thinking about the action research group. I have come to see a critical action research project as more open and fluid, as a ‘self-constituting public sphere’, and to see those who participate in the shared project of a particular programme of action research as engaged citizens committed to local action but with a wider critical and emancipatory vision for their work. The critical action research group might thus be understood in relation to, and as a contribution to, wider processes of social movement (Kemmis, 2001, p. 101).

Action research inquiry is therefore progressive from technical to practical, and then to emancipatory. It allows both the participants and the researcher/practitioners to learn and experience through the action research cycles, and emancipates and
transforms both their practices and organization systems progressively. This is an important strength of the methodology.

In the context of this study, organization ALPHA was a multi-national corporation that has many established policies, processes, and procedures that were being followed and practiced for many years. Introducing change to the existing systems naturally faced resistance. As such, a progressive approach was necessary, both to allow for any changes to the systems to be introduced as a learning process, and for the researcher-practitioner to learn from the work in both the research and practice areas progressively. Existing tools and processes familiar to people in the organization can also be adopted or adapted without reinvention, whenever possible. With careful and explicit negotiation of the roles of researchers and other stakeholders participating in the research, adequate visibility of the actions that management and staff would be more interested in addressing could be established without compromising the purposes and quality of data collection for the research. From the methodological standpoint, this provides opportunities to achieve a good balance to attain the desired research quality.

3.2.3.7 Socio-technical human activities systems

Information security problems are not just technology problems. It is often said that people are the weakest link in the information security chain (Mitnick et al., 2002; Schneier, 2003; Viega, 2005). Information security systems failures are often due to people's failure to recognize risks, manage risks, and operate systems securely to prevent risks from happening. For information security management, we therefore see an evolution into information risk management, which is more encompassing, taking into consideration the people, process, and technology aspects involved in information systems (Mahtani, 2004).

As described in Pasmore (2001), Kurt Lewin’s field theory, which stated that “the behavior of an individual is a function of both personality and environment, demonstrated that behavior varied across time and under the influence of different environmental forces”. The socio-technical school also believes that behavioral changes could be produced by changing aspects of the workplace. From a socio-technical perspective, “no matter how advanced the technology, it would fail if not mated with a social system designed to operate the technology effectively”. This is
known as the principle of “joint-optimization”. Tracing the historical development, accomplishments, and evolving theories and practices resulting from action research and socio-technical approaches, Pasmore concluded that “the practical and theoretical contributions of the two groups were so closely aligned that it would be more sensible to describe them as one school of thought rather than two” (Pasmore, 2001).

As established in Chapter 2, both social and technical factors are co-producers of the intended outcome of information security risk management. The distinctive characteristic of each must be respected, or else their contradictions will intrude and their complementarities will remain unrealized. Action research, which is inherently aligned with the school of thought in the socio-technical approach in social research, is therefore relevant and suitable for studying information security risk management systems. The use of action research will enable the people aspects of the challenges to be studied without disregard for the technical nature of the systems environment involved. Action research cycles include people as participants and co-researchers. The cyclical process will ensure that the people’s gaps and issues are observed and critically reflected in the respective action and research, thus, providing a better understanding of contexts, situations, and reasons for the existence of these gaps between people and systems in the information security chain. Soft Systems Methodology (Checkland, 1999; Checkland & Holwell, 1998; Checkland & Scholes, 1990), a category of action research, in particular, emphasizes the “soft” side of the systems, i.e., the human activity system.

3.2.3.8 Systemic thinking and action research

As highlighted in Dick (2001; 2002a), one of the profound values of action research is its responsiveness and flexibility. They are inherent in its design (Section 3.2.3.4), its close alignment with the socio-technical approach (Section 3.2.3.7), and its suitability in a variety of situations from technical, practical, to emancipatory (Section 3.2.3.6). Beyond this, the value of action research has also been recognized in the domain of systemic thinking.

According to Robert L. Flood, systemic thinking is grounding that can “broaden the action and deepen the research” in practice. “Systemic thinking assumes that the social construction of the social world is systemic, which means that phenomena are understood to be an emergent property of an interrelated whole” (Flood, 2001, p. 133).
A systemic view of the world is characterized by emergence and interrelatedness. “An emergent property of a whole is said to arise where a phenomenon cannot be fully comprehended in terms only of properties of constituent parts.” It is the cognitive interpretation made through the process of the human brain that provides the understanding of social phenomena. A systems approach employs concepts like emergence and interrelatedness to interpret social phenomena, rather than to represent systems as if they exist in the real world. It entails qualitative and/or quantitative modeling of the social systems to describe or explain a social phenomenon or predict events and suggest actions for improvements.

Such a systems approach might be particularly empowering in this endeavor of meaning construction if the world is indeed systemic. That is, such a systems approach promises to construct meaning that will resonate strongly with people's experiences within a systemic world (Flood, 2001, p. 133).

Action research carried out with a systemic perspective in mind promises to construct meaning that resonates strongly with our experiences within a profoundly systemic world (Flood, 2001, p. 144).

Soft Systems Methodology (SSM), as described in Checkland and Howell (1998), provides an approach that is inherently systemic. It has been used extensively in research relating to information systems. According to Flood (1999, p. 60), “the link of [information systems] to SSM is that people undertaking activities in a human activity system always need information support”.

Clearly, action research in the field of information security risk management, undertaken with a systemic perspective, will provide significant opportunities for more learning and knowledge contribution to both domains.

The advantages of being a meta-methodology, a process-oriented approach, with inherent inclusion of people and the social aspects of systems, and the combination of change (action) and understanding (research) suggest the relevancy, and therefore make action research an appropriate methodology for this research study.

3.2.3.9 Limitations and resolutions

Although action research has clear advantages in its application in this research context, especially when it is designed to be conducted in a changing organization, it
has its share of shortcomings in which this research should be mindful of. This sub-
section highlights the potential issues and challenges, and steps taken in the research
design and execution to manage, if not address them.

Gill and Johnson (2002) highlighted two main concerns from the methodological
perspective. They are (1) the difficulty of evaluating action research; and (2) the
ethical dilemmas involved in action research.

In considering the difficulty of evaluation, Gill and Johnson highlighted concerns over
the formal recognition of action research in the eyes of positivist researchers. They are,
however, not an obstacle per se. The notions of praxis, hermeneutics, existentialism,
pragmatism, process philosophies and phenomenology have shown action research as
science by locating its foundation in philosophical viewpoints that differ from those
used to support positivist science. In applying action research to this study, it is
therefore important to ensure that these notions are addressed, and the dialogical
view\textsuperscript{66} of action research, where researcher and organizational members are treated as
equally knowing participants, results in a different epistemology that produces a
different kind of knowledge of use to a particular organization and/or the information
risk practitioner in a similar or near-similar context or environment to that of the
research (Gill & Johnson, 2002, pp. 92-93). Dick, Passfield, Sankaran, and Swepson
(2001) have also presented ideas of similar thread, which therefore lend further
credence to the action research method used in this study.

Gill and Johnson (2002) suggested three other dilemmas for considerations in action
research. First is the acceptability of the client to the researcher, for ethical reasons.
We will defer our detailed discussion of the ethical aspects of the research to Section
3.4 below. Briefly, the ethical requirements for this study were minimal and
manageable, given that no personally identifying information was captured, and the
emotional aspects of people involved were not within the scope of the study, although
there may be merit for such an evaluation in a future follow-up to this work.

The next two concerns are the confidentiality and protection of respondents. These
were relevant to this study. Two aspects of confidentiality were considered – the
confidentiality of organizational information, and that of personal privacy, character
and behavior, with regard to respondents and participants in the study. Organizational
information relating to “weaknesses” or “gaps” identified in the course of the study
was a potential source of confidentiality concerns as they might have an impact, directly or indirectly, in terms of the organization risk status as perceived by its clients and regulators where it operated, should such information be revealed in a manner that was not carefully managed or communicated. However, as the risk environment is constantly changing, data captured during this study would be obsolete by the changes that have taken place upon this dissertation. Respondents or participants’ confidentiality were assessed to be less significant as they were less permanent, but exercising due diligence in the study to protect them remained relevant and important in order not to invite a negative outcome that can be prevented with a little more care in the handling of the related information. In view of these concerns, names of the organizations and people involved in this study were replaced to obscure and protect their identities. Unlike other non-organizational based type of research, wherein information protection mainly takes place during the research itself, but not after its completion, the publication of the action research outcome has to take into consideration confidentiality and protection requirements, at least for a period of time after the completion of the research in order not to create any ethical dilemmas.

As an insider action researcher, there was also a risk of bias when I entered the research with a perspective drawn from my own past experiences. Herr and Anderson (2005, pp. 60-61) however assessed this as “natural and acceptable in action research as long as [past experiences] are critically examined rather than ignored”. In this study, in addition to the use of triangulation and multiple sources of data to improve validity, this was addressed by having a critical reflexivity in the research process, and, more importantly, having “validation meetings” held with critical friends and other action researchers from the learning set (see Section 3.3.3.1) to get a range of different responses to my findings and understandings. These helped me to reflect on my practice and validate my research claims.

From the research perspective, there was no known *a priori* application of action research in the field of information risk management. This means that the use of the action research paradigm in this study was experimental, and not all actions planned might work the first time. There was a risk that the research paradigm or selected methodology for each stage in the cycle might not work as intended, leading to a prolonged research period, or an unexpected outcome requiring more resources than available or anticipated. There were no directly relevant cases that can be used as
references to give hints for planning the next step as well. These limitations, however, may also be viewed as an advantage, as they provided more room for creativity and discovery than would have been possible with a safer path. What this meant was that there was a need for more diligence in following an established process of the chosen methodology within the action research paradigm.

3.3 Research Procedures

The beginning of the field work for this study coincided with the starting of my employment with organization ALPHA on January 2, 2002, as a Regional Information Risk Officer (RIRO), undertaking the responsibility of managing the Information Risk Management (IRM) program for the organization in the Asia Pacific (AP) region. This included managing a 10-member team, monitoring and maintaining the related risk management processes and tools, and dealing with the challenges in all these aspects. It was not a new function, but an evolving one that incorporated several different practices by different parts of the then newly merged organization. My role as an action researcher was negotiated and approved by my supervisor, and made known to three key participating members of the regional IRM team. The team members were receptive and supportive of the study. Throughout the process, they provided regular, prompted and unprompted, feedback on the changes and actions that were taking place, their reflections, and issues, resolved and unresolved. This combined role (of action researcher and practitioner) in ALPHA ended in August 2003 when I left organization ALPHA and joined organization BETA. At this stage, a substantive theory for information security risk management has already been induced from the analysis of the data collected, and critical reflection conducted in ALPHA. This was the end of the first phase of the study.

In organization BETA, my role was a regional security advisor (SA), responsible for providing professional advice to help Information Security Risk Managers and related or equivalent roles in BETA’s customers’ organizations develop their security strategies and plans, and to manage the execution of those plans to achieve similar objectives to those in my previous role as a RIRO in organization ALPHA. My role as an action researcher continued in parallel as the regional SA of organization BETA. This was approved by my supervisor in organization BETA. In this role, my research focus shifted towards collecting new data based on critical security incidents faced by organization BETA, and also interviews with BETA’s customers and information
security risk managers in other organizations to seek negative cases and disconfirming evidence to the findings and theory induced from the results of the action research conducted in organization ALPHA. This has included a survey-led questionnaires and interviews with 30 practitioners, case studies of security incidents and focusing events, validation testing of the derived approach in organization CHARLIE, and open dialogue and discourse of the derived approach in discussion forums and industry conferences in the AP region. This was considered the second phase of the study, which ended with the completion of the writing of this thesis.

This section describes the strategy and processes within the action research cycles undertaken for data collection, analysis, and interpretation throughout the period of the study.

### 3.3.1 Action Research Cycles and Stakeholders

From a meta-methodology perspective, the research study consisted of six sub-cycles within four major action research cycles as shown in Figure 5.

![Diagram of Action Research Cycles](image)

Figure 5: A meta-methodology perspective depicting the four main research cycles encompassing the seven sub-cycles

Each of the four major action research cycles carried a theme that progressively led to the completion of the study. The four main action research cyclical steps within each action research cycle include the following primary research activities are described in Section 3.3.2. The main themes that evolved from the four main action research cycles are:
AR1: Understanding the System - The first action research cycle, which was an initial reconnaissance phase, was about learning and understanding the information risk management practice, and the related systems and people in ALPHΑ. The Kemmis and McTaggart’s (1988) “Action Research Planner” was selected and used (as it was one of the more prescriptive guidance on conducting action research that I found from my literature review, in particular, in the initial reconnaissance phase) to identify the key attributes of the environment, internal systems and people in the organization. At the end of this research cycle, the issues and dilemmas of the risk management approach in organization ALPHΑ, which was largely control-oriented and compliance-driven, were identified and the notion of “piezoelectric response” emerged.

AR2: Model A approach – The initial cycle was followed by a “do something different” cycle, whereby a system change was designed and introduced to the organization. The objectives of this cycle were to gain further understanding of the information risk management systems involved, and begin the process of developing an information risk management model (known as Model A) for the questions relating to this study, to address the issues and dilemmas identified. Based on the understanding of the organizational and information risk management systems provided through the earlier sub-cycles, several key problems were identified. As practitioner in the organization, from a management perspective, these problems needed solutions. The next sub-cycle—“solve the problem”—was therefore initiated to focus on improving the plan and using action research methods to apply it to the problem areas. Improvements were made to the model based on the learning gained. The outcome of these sub-cycles was analyzed as part of the data analysis process to provide further understanding for the research objectives. Model A approach provided a comprehensive system for managing information risk in organization ALPHΑ, addressing the social-technical issues and dilemmas identified in the earlier research cycles, but was found to still lack the elements required to deal with unplanned changes, in particular, relating to security events that were unanticipated in the risk assessment process.

AR3: Model B approach – While Model A was stabilizing in the organization in the Asia Pacific region (where the research was conducted), senior management decided to re-organize the information risk management function globally.
The re-organization introduced several changes to the regional organizational structure, reporting line, and roles and responsibilities. This provided an opportunity for Model A approach to evolve to support the planned change, and also adapt to a distributed organization structure. A new action research cycle was therefore invoked to implement and manage the new change, focusing on implementing the evolved model (named as Model B approach) to address the outstanding issues and dilemmas left over in the earlier cycles. Nevertheless, the outcome of this research cycle disconfirmed the suitability of Model B approach for addressing the issues and dilemmas relating to the research questions. It further established that the solution to the research questions was not in the organizational structure, or the incorporation of social science techniques in the risk management process, although they did improve the understanding and effectiveness of the IRM involved (see Section 4.3.2).

AR4: Responsive approach – The findings from the development and testing of Model A and Model B approaches asserted that both approaches were inadequate to meet the needs of the changing risk environment, even though some of the issues and dilemmas identified in the initial research cycle can be addressed. To address the needs of the changing risk environment, the research was redirected towards development of an approach based on the concept of “piezoelectric”, which had earlier emerged as a plausible metaphor for approaching information risk management issues with a new perspective. The concept led to the derivation of a substantive theory, known as “piezoelectric theory of information risk management”. The outcome of the piezoelectric theory is the notion of responsiveness. The implications of responsiveness was found from interpreting the analysis of a case study conducted in organization BETA, and further observations, analysis, and interpretations of the series of security and catastrophic events that emerged during the period of this study. Model A approach was improved to cater for the responsiveness requirements and named as the “Responsive Approach”, and implemented for validation testing in organization CHARLIE (as described in Section 3.3.3.3). The responsive approach implemented in organization CHARLIE demonstrated a resolution of the issues and dilemmas identified in the earlier research cycles, which in conjunction with the findings from the case studies, supported the validity of the piezoelectric theory.
The findings of the four major action research cycles were further analyzed and interpreted against the research questions resulting in the final refinement of a substantive theory for information security risk management, covering the key attributes, and a framework and methodology suitable for use in the practice environment, as described in Chapter 4.

3.3.1.1 Stakeholders

The main stakeholders in the study, besides me, as the researcher and practitioner (participant), include:

- Research supervisor and co-supervisors, whose interest and focus were to ensure that I conduct the study as per planned, use the action research methodology and other research methods and tools appropriately in the study, and carry out critical reflection as and whenever possible, and at the end of the cycle. As such, they were involved in reviewing the plans at the commencement of each action research cycle. At regular interval, critical reflective sessions were conducted between the supervisor/co-supervisors and I to review and reflect on the action research steps executed, the outcomes of those steps, the plan for improvement and subsequent steps, and the results of my critical reflections. Their contributions in the reflective session helped to sharpen my thoughts, reflections and subsequent actions, and therefore had positive influences to the outcome of the study.

- Research collaborator. The research collaborator played a key role for me to bound-off ideas, and ascertained that my plans and actions at each stage were on track in terms of the research practice. At regular interval, critical reflective sessions were also conducted between my research collaborator and I to review and reflect on the action research steps executed, the outcomes of those steps, the plan for improvement and subsequent steps, and the results of my critical reflections. My research collaborator often shared his experiences and knowledge on using action research in research and practice, which helped in ensuring the appropriate use of action research methods, and over and above his responsibility, often reminded me of my progress and ensure that I do not put-off the research activities as a result of work pressure. The research collaborator’s contributions throughout the study, and in particular,
in the reflective session helped to sharpen my thoughts, reflections and subsequent actions, and therefore had positive influences to the outcome of the study.

- Participant (me) – Besides being the researcher, I was also an active participant (practitioner) involved in the execution of actions in the field itself. During action research cycles 1, 2, and 3, while I was with ALPHA, my role as a participant was directly involved in translating the research plan into field plan, and executing the planned activities in the practice environment. In action research cycle 4, when I moved to BETA, as highlighted earlier in the introduction in Section 3.3, my role as a participant changed slightly in that I was the advisor providing information and knowledge and influencing the actions of other participants in taking most of the actions related to the practice (not the research role, such as conduct of interviews and note taking though), while I was also actively collecting available data for the case studies. The implication of this slight change of role as being a passive participant in CHARLIE was that the actions taken and results reported was through the other participants (i.e., the CSO and his team) who executed those planned actions. As such, the outcomes of the actions were from the follow-up interviews, rather than direct observations of the execution. Given that there were few issues involved in the execution, I assessed that this arrangement did not have significant implication to the final outcome.

- Participants (team members, colleagues) – these participants were staff members of ALPHA and BETA, as well as those of CHARLIE (and their contractors) who were interviewed as part of the research steps executed. As the approach taken was focusing on improving the problem situation in the work environment, which was their main interest, even though they were aware of the study, the participants did not regard the study as a significant aspect of the actions involved. They were comfortable providing feedback and discussing their thoughts during interviews and the critical reflection sessions. As such, their appointments and participations did not present any difficulty to the study, and hence assessed as having insignificance implications to the final outcomes, even though the data that they have provided did contribute to the outcomes.
• Participants (customers) – the LOB staff members and managers in ALPHA, and business customers of BETA, which include CHARLIE, were participants in a few steps of the actions and reflection aspects of the related cycles. Similarly, these participants were focused on improving their problem situation rather than the study, and were comfortable sharing their thoughts during interviews and reflection sessions held. While these participants contributed to the study from the participation, their views and contributions were not found to be influenced by the positions that they held in the organization. As such, they do have significant negative implication on the outcomes, even though the data that they have provided did contribute to the outcomes.

• Participants (other practitioners, neither customers nor colleagues) – these were participants who neither work for ALPHA, BETA, CHARLIE, nor BETA’s customers, but information risk professionals outside of these organizations. These participants were part of the respondents to the information risk management survey. They were briefed on the objectives and use of the survey and related study, and consented to the ethical and privacy policy stated in the consent form for the survey. As they were also not members of the organizations that I was working for, their responses were assessed as objective, and therefore no negative impact on the data-driven final outcomes.

• Managers – These were my managers in ALPHA and BETA, who supervised my plans and actions from a business practice (non-research) perspective. While these stakeholders supported the conduct of the study, they did not have a direct stake in the study. However, the plans and actions that I developed and executed were strongly influenced by the action research processes that I practiced. The efficacy of my study was therefore important from the business perspective. These stakeholders were interested to ensure that I have an effective, efficient, and actionable plan (from the business perspective), and the actions taken were also effective and efficient, achieving the desired business outcomes. As the study was workplace related, I have to work within the boundary and constraints of the business requirements. As such, the business directions and decisions made at the managers’ level did
have impact on the progress and outcomes of the planned study and actions. They were therefore regarded as participants, and their actions and decisions were observed and analyzed as part of the research data collected. Nevertheless, these stakeholders did not block the progress and execution of the study and related actions, and therefore did not create any significant impact on the study.

- Non-stakeholders – These were non-participants who were not involved in the study. In the context of the study, they were professionals in the IT and information risk management industry who provided impromptu feedback in the conferences, seminars, and roundtable events that I participated and presented, on the findings of the study, and the substantive theory that I have developed. Their views and input were assessed as objective as they were impromptu, responding to the discussion and presentation that I facilitated or presented, in which they were first time receivers of those information.

### 3.3.2 Action Research Process

Based on the research process described in Perry and Zuber-Skerritt (1992), as depicted in Figure 6, within each action research sub-cycle described in Section 3.3.1, I applied an action research spiral process (Spiral A) for data collection and literature review, and, in parallel, another action research spiral process (Spiral B) for interpretation and reflection of these results, documentation of the research outcomes, and writing the research report.

When the study was initiated in January 2002, my first priority was to understand the environment, identify the key stakeholders, and obtain an inventory of all the things (hard and soft) that I had inherited before determining suitable actions for the first action research cycle. Using Kemmis and McTaggart’s (1988) “Action Research Planner” as a guide, I drew a project plan consisting of the four main phases, plus an initial reconnaissance step for gathering initial information, and identifying thematic concerns (in IRM areas) of the firm in the region. The tool for identifying thematic concerns – the “Aristotelian Table of Invention”68 – as described in Kemmis and McTaggart (1988, pp. 91-99), was also adopted as part of the initial reconnaissance step.
Kemmis and McTaggart’s (1988) “plan-act-observe-reflect” (PAOR) process, which has provided a comprehensive step-by-step method for starting an action research project, was adapted within the individual action research spiral.

Each spiral was designed to be cyclical so that data from multiple and different perspectives could be gathered to triangulate the results, and to confirm or disconfirm the findings for better understanding of the organizational environment, related changes, and identifying key information risk management issues gained through the research.

The outcome of each cycle in Spiral A, through the reflection phase, was fed into the thesis writing spiral, or Spiral B, again at the reflection phase. In Spiral B, reflection from the outcome received from Spiral A resulted in modification of the thesis writing plan, and the theoretical thinking and conceptualization around the topic of the thesis, which then initiated the next cycle of writing. At the action phase of Spiral B, which
involved compiling material and drafting, new ideas, questions, or information requirements were generated. Gaps in earlier thinking and findings from Spiral A were at times identified. All this was converted into requirements for more data and understanding from the fieldwork, which therefore influenced the planning phase of the next cycle in Spiral A. This inter-switching of the two Spirals coincided with the switching of hats by me from being both a participating practitioner and an action researcher.

In practice, I undertook the following activities for the four main action research steps of the two Spirals:

- **Plan** – This included identifying the stakeholders of the study and in the organization where the actions were to be performed (namely, ALPHA, BETA, and CHARLIE), conducting the stakeholder analysis, planning for data collection, selection of data collection methods (which was predominantly interviewing and documents reviews), and scheduling the activities.

- **Act** – Executing the planned activities, including presenting my role and the functional organization I was representing, objectives, and program that I was running, to the participants; interviewing the participants; listening to their feedback; reviewing historical documents; taking notes; journaling; conducting stakeholder analysis on the organization in relation to the planned actions; and following-up to related activities on-the-job.

- **Observe** – Reviewing the activities logs, journals, meeting records, and observing people’s behavior within my organizational function (in particular, the IRM function in ALPHA), among the external stakeholders (participants), as well as around the organization in general. The aim of these reviews was to look for any obvious patterns, signs of change, and related events and critical incidents that might have occurred during the period, either as a result of the actions taken, or other external factors, which may be positive, negative, or neutral to the study.

- **Reflect** – This involved analyzing the data collected (including the observations recorded in the journals) looking for critical incidents, critical reflection over the outcome of the analysis, identifying negative cases and disconfirming evidence, by myself, with my research collaborator, with the
AR Learning Set, and with my research supervisor and co-supervisors to develop my analysis, triangulate my understanding, theorize the practice, and improve my practice. While in ALPHA, reflective sessions were also conducted with the IRM Learning Set that was established with the IRM members to reflect on internal IRM practices. In addition, critical reflective sessions were also held with my managers and team members to reflect on the outcomes of actions from the practice perspective, and determine follow-up actions necessary for improving future outcomes.

### 3.3.3 Data collection, Analysis, and Interpretation Procedures

This sub-section describes the methods that were used for data collection and interpretation for the study within the action research cycles and process described above. It explains how I used the data collection and interpretation method to maximize the chances of good understanding and effective change, identified the shortcomings of the method for the purpose, and explains how I compensated for them in the execution of the research and action.

#### 3.3.3.1 Data sources and validation

Multiple sources of data were used in the research through the respective phases or cycles of action and research. The aim was to increase rigor of the research, and to provide different perspectives that could challenge the findings, “focusing on agreements and disagreements and ignore the more idiosyncratic data in any data set” (Dick, 1997c, 1999a, 1999b).

#### 3.3.3.1.1 Interviews

Interviews, which included face-to-face and phone interviews, were one of the main methods for data collection.

Two forms of interviews were conducted. Interviews in the initial phase were conducted mainly in the form of meetings, as part of my practitioner role (as a RIRO) for the company in the Asia Pacific region. The process of a “convergent interview”, as described in Dick (2002b), was adapted. Convergent interviewing is systematic, easy to be adopted, and flexible to enable use in complex or confusing situations. The adaptation was necessary in view of my practitioner role, which requires the sessions to be interactive, rather than structured traditional interviews.
Chapter 3 – Research Methodology

The participants were informed of my objectives and agenda for all the meetings – to understand the current situation and issues that they faced, establish their understanding of the situation and issues in and around the information risk management function, and devise actions to bring about effective change that would benefit them in return.

As meetings, the interviews involved more information sharing and dialectics, which “craft agreement from disagreement” (Dick, 1997a) than traditional interviews. The interview/meeting sessions allowed me to market my roles and responsibilities, what I was there to achieve for the stakeholders, and my current thinking and plans. Using a dialectic approach, I focused on any disagreements that might exist in the session, and sought to turn them into agreements to gain greater understanding as a result of the sessions. The disagreements/agreements may not necessarily be from the participants, but also me as one of the stakeholders/participants. This approach allowed more information sharing and consensus building to occur almost concurrently, instead of just information gathering, which would face more resistance in an organizational context.

Critical reflections were conducted at the end of each meeting, and journals were written to document key attributes, reflections, and follow-up actions devised as a result. Pseudo-names were used to denote participants, to provide anonymity and to ensure their privacy.

The second form of interview, which was used in Phase Two of the study (after August 2003, in organization BETA), also adopted the style and process of convergent interviewing closely. Interviews conducted in this phase involved mainly external participants.

An initial set of questions was devised before the interview process began in each of the two phases of the study. In Phase One, the questions focused on (1) what is the business of the stakeholder/participant involved; (2) what are the (perceived) information risk to their business; (3) what do they understand about information risk management in the company, and in relation to their business; (4) what are the issues and concerns with the current information risk management function that they have been dealing with or dealt with before; and (5) what are the desired changes or clarity (understanding) that they would like to see going forward?
In Phase Two, the questions focused on two areas. One was to follow-up on the mini-
survey to verify participants’ responses; determine the information security risk
management practices in their organization; their role and responsibilities as
information security risk manager; current challenges in managing information
security risks; outlook on possible future directions; how those challenges might be
resolved; and gain further insights into the issues, dilemmas, and practices in their
organizations. These questions were based on the mini-survey questionnaire
(described in Section 3.3.3.1.4) for Phase Two. The other area of interviews focused
on the concept of responsive security, based on the principles of “piezoelectric”,
which was the substantive theory developed from the outcome of Phase One. The
purpose of these interviews was to seek disconfirming evidence to determine the
applicability of the “piezoelectric” principle and associated concept of responsive
security.

3.3.3.1.2  Note Taking
Note taking was the primary means of data recording – voice recording was not used
in the initial period. It was later introduced as the number of telephone
conferences/meetings increased—those that occurred in the evening with colleagues
in New York and London, and as the subject matter discussed started to expand in
scope and increase in depth. These methods, using typewritten notes and voice
recording, are most efficient for capturing large amount of data.

Cautionary steps were taken in the research documentation to ensure that the privacy
of the individuals involved was not revealed. This included changing the personal and
department names to pseudo-names. As highlighted in Williams & Harris (2001),
“you don’t know what data might be relevant to your reflection until you start
reflecting”. Critical reflection was conducted usually at the end of each day, at times
over a few days or at the end of week, as I changed my hats from that of a RIRO to
that of an action researcher, using the written notes and voice-recorded memos taken
as research data, observing, and performing reflection for gaining understanding,
refining the initial research questions, and deriving new questions to further the
inquiry into the IRM domain in the Firm. Journals were written as part of the
reflection process (as described in Section 3.3.3.1.8).
3.3.3.1.3 Historical Information and Working Documents

Historical information about IRM functions and work done previously that were captured in the company databases maintained by the respective heritage organizations form another source of data that provided insights and understanding on how things work previously in the company.

Working documents including minutes of meetings, internal reports, relevant electronic mails (emails), and documents hosted in internal organizational Intranet web sites were also used as additional data sources to provide further understanding and evidence of occurrence of specific incident that were of relevance to the study.

3.3.3.1.4 Survey

A mini-survey was conducted, including 37 questions (see Appendix A), for a group of 30 external participants. The purpose of the survey was to serve as a basis to collect initial data to guide the follow-on interviews (Section 3.3.3.1.1) with the participants to gain understanding of the organization’s practices and key issues to triangulate and seek disconfirming evidence of the findings of the first two years of the study conducted in organization ALPHA. Personal data were not collected in the survey.

The questions were categorized into six parts. Part one was designed to gain a general understanding of the demography of the respondent’s organization and his/her role within. As the purpose of the survey was to gain understanding of the organization’s practices and key issues, but not the respondents’ personal feeling and behavior in the organization, gender and age of the respondents were assessed to be irrelevant. In accordance with the privacy principle of collecting only relevant information, age and gender data were therefore not collected in the survey. Part two was designed to collect data regarding the setup of the information security organization. Part three determines the organizational policy and general practices in information security risk management. Parts four and five sought to determine whether other organizations recognize the critical need to manage and get ready for information security incidents and the role of the information security function during and after an incident. The final part was designed to elicit the respondents’ views on key emerging practices that were identified as significant developments for dealing with changes in the risk environment.
Chapter 3 – Research Methodology

The selected sample of 30 participants was all in an information security risk management or related role similar to my role in ALPHA. The sample size was constrained by the limited number of individuals in the Asia Pacific region who have similar roles in organizations, as the role was only recognized in very recent years as important for managing information security risks in organizations (Kowalski, 1995; Mahtani, 2004). The small sample size, however, allowed follow-up interviews to be conducted to clarify responses and ensure the accuracy of the data collected. This further served as an entry process (Dick, 2002c) for building rapport with the respondents for subsequent validation interviews on the derived framework and methodology for information security risk management. The survey was tested with 5 CSOs (from a number of countries in Asia) in conjunction with the execution of a security roundtable event in Korea and Singapore in 2004, whereby the questions were corrected for grammatical errors and improve readability before the survey was rolled out in 2005. The interviews were conducted as described (as the second form of interview) in Section 3.3.3.1.1. Results of the survey form part of the data that are used in the analysis and interpretation of the observations and emerging themes from the action research cycles conducted, as presented in Section 4.2.1, 4.2.2, 4.2.5, 4.4.5, and 4.4.6. The consolidated report of the survey with breakdowns on the type and roles of respondents and correlation of their roles to the responses provided was recorded in J20061029. The identity of all respondents was kept anonymous in the study.

3.3.3.1.5 Learning Sets

A learning set, as described in Dick (2002d), is a face-to-face learning group with which a researcher can discuss his or her work. Two learning sets were used in this study.

One of the learning sets consisted of three local co-supervisors and six PhD research students, including myself. In 2004, the number of co-supervisors grew to five, and research students increased to eight. With co-supervisors who are skilled in facilitation, monthly meetings for the learning set enabled members from different situations to help each other learn. The various learning sets included open dialogues on each member’s action research project and key incidents encountered based on his or her problem situation. Through participation in the learning set, my understanding
of the philosophy and practice of action research relating to my problem situation increased as well.

The supervisor team, as the name implies, was an academic group consisting of two supervisors and one co-supervisor from Southern Cross University. The supervisor team oversaw each candidate’s overall academic performance and research progress. In addition to email facilitation, they provided face-to-face discussions over a week-long interacting workshop every six months.

Another learning set was established nine months after the initiation of the study in ALPHA, with members of the Asia IRM team as learning set participants. A monthly session was conducted including open dialogues to improve information sharing, and increase individuals’ competency in the IRM role and skills through knowledge transfer on a rotational basis. The internal learning set provided valuable sources of data to further enable its members to understand the issues, concerns, and challenges relating to individual participants, which helped me to further understand the problem situations and chart new directions in the action research cycles.

3.3.3.1.6 Conferences, Seminars, Roundtables and Workshops

Outcomes of the research following the completion of Phase One, and during the course of Phase Two (since November 2003), were also presented in numerous public conferences, seminars, roundtables, and workshops where the topic of information security risk management was discussed, to share knowledge and further invite public discourses progressively on the substantive theory induced from the research. For example, see Kang (2005a; 2005b; 2005d; 2005e; 2005f; 2006a; 2006b; 2006c; 2006d). This provided an additional venue to further seek disconfirming evidence to validate the research outcome.

Through these security events, I have shared knowledge of the responsive approach with more than 1,000 public audiences, and discussed its principles and methods with numerous senior information security practitioners and government officials.

These public presentations also served as a platform for contributing my learning to the learning of fellow practitioners. With one presentation learning from the sharing and feedback received from the previous, they were one of the vehicles where I continued my enquiry, supported the validation of my theory of practice, and contributed to my information security risk management practices and strategy. In
addition, those platforms provided a way to improve the learning of other practitioners and managers when I shared how the responsive approach was derived through action research practices, and encouraged them to become action researchers and be critical and to find ways of practicing that are educational for themselves and their fellow colleagues. My role in these events was therefore in both transmission mode (in which I shared my knowledge and understanding on information risk management and the needs for responsiveness) and dialectics, in which the participants, who were mostly information risk management stakeholders, provided feedback on their issues and dilemmas, the model proposed, as well as explored ideas on possible approaches for implementation.

3.3.3.1.7 Literature

Literature is a valuable source of information to provide support or disconfirmation of relevant research findings, and as such, can be thought of as data (Dick, 1999a, 1999b). Literature search and reviews were conducted as part of the action research cycle in the planning, and reflection stages in the field work cycles, as well as part of the data analysis and interpretation process in the thesis writing cycles (c.f. Figure 6).

3.3.3.1.8 Journals

In addition to the above, I have kept a set of journals of all critical reflections, observations made, and minutes of meetings since the start of this research in January 2002. Each of these research journals has been catalogued in the “Research Log Register” in Appendix B.

3.3.3.1.9 Secondary Data Sources

Secondary data sources used were publicly available media reports, newspaper articles, and reports of public surveys conducted by industry-recognized organizations in the field of information security.

3.3.3.2 Data Analysis and Interpretation

Data analysis occurred throughout the action research cycles as part of the critical reflection process in the field work, thesis writing, and literature reviews (as shown in Figure 5).
Chapter 3 – Research Methodology

The research was designed as a data-driven action research (Dick, 2000b), with the aim to evolve the research design and procedures into more details in a progressive manner, based on the data collected from each action research cycle conducted. As highlighted in Dick (2000b), “this can provide some protection against the biases and preconceptions which researchers and others inevitably bring to the research situation”. As such, data-driven analysis was used extensively in the research.

As described in Tripp & Wilson,

It can be taken as axiomatic to action research that to achieve good outcomes we have to understand our existing practice in order to identify ways to improve. To do that we have to systematically examine our normal ways of practicing and problematise what we’re doing and its implications. The production of critical incidents from entries in self-reported observation journals is an effective way of generating such understanding (Tripp & Wilson, 2001).

As part of the data analysis process, I therefore reviewed the research journals to identify critical incident from the events captured so that performing critical reflection over those incidents could help to (1) develop my analysis, (2) theorize my practice, (3) improve the outcomes in subsequent cycles, and (4) develop personal-professional practice (Tripp & Wilson, 2001).

Critical reflection, reflecting on the actions against plan and observed outcomes, focusing on critical incidents, further involved seeking of disconfirming evidence, using triangulation of data from different sources and negative case analysis (see Section 3.3.3.2.6).

The following sub-sections describe the selection, design, and execution of these methods that I had applied in the study.

3.3.3.2.1 Data-driven Analysis

The method of data-driven analysis as described in Dick (2000b) was adopted in this study. As shown in Figure 7, data analysis began with taking any two or more sets of data that have been collected, starting with those having disagreements. These data may be collected from different sources, using different methods, from different groups or participants, conducted at different times, or in different situations. The disagreements were then noted (written down), and explanations were sought for the disagreements. Any agreements (apparent or specific) were also noted, and exceptions
to such agreements were then sought after. Exceptions, when found, were examined to see if they disagree with former agreements, which could therefore turn previous agreements into disagreements. Through this process, the deeper understanding achieved was then used to determine the next course of action. The results of the next course of action were fed back to the data-analysis process in the next action research cycle to gain further, and deeper, understanding.

In conducting this study, data analysis commenced after the initial round of interviews with the initial objectives to identify key agreements, exceptions within agreements, and disagreements among the participants within specific groups of stakeholders and participants, and between different groups. From this, better understanding of the issues of the function and people engaged in it evolved. In a form similar to convergent interviewing, the results were applied to add more specific probes to the set of basic questions in the subsequent interviews to identify further agreements, exceptions to agreements, and disagreements.

![Diagram: Data-driven analysis - seek disagreement and exceptions to gain better understanding and better actions (Dick, 2000b).](image)

For example, in Phase 1, from a list of disagreements identified in basic tasks executed by the auditors and IRMs, a common agreement that evolved from an initial series of meetings and interviews was that the audit function was inconsistent in its assessment of the business information risk. The inconsistency existed within the audit function, and also between the audit function and the IRM function. IRM played a role to help bring about consistency in this regard. Another issue agreed upon by a number of participants was the role of IRM in an audit situation. To seek more understanding on the audit versus IRM roles, auditors’ consistency of practice, and
the role of IRM in an audit situation, these issues were used as probes in subsequent interviews to determine if they agree, agree with exception, or disagree with the initial findings, and their rationale for their respective stand on the issue. The findings were further discussed with my team members to seek their feedback for triangulation, and possible disconfirmation, thereby confirming and disconfirming respective explanations before devising follow-up actions for the next research cycle.

The process of data-driven analysis conducted in each of the action research cycles focused on identifying disagreements and exceptions, and seeking explanations to gain a greater understanding leading to better actions in subsequent cycles. Combining the data analysis process with the procedures of action research, involving note taking (as part of planning and observation), and journaling (as part of critical reflection), the methodology adopted closely matches the steps of grounded theory (Glaser & Strauss, 1999). As noted in Dick (2000c), this can be regarded as a “variation” of the grounded theory using action research, which is also “more responsive to the research situation”.

3.3.3.2.2 Causal Mapping

Causal diagrams were also used in the study to provide structure to the qualitative data to facilitate analysis and understanding. The causal mapping and analysis technique as described by Peter M. Senge (1990; 2006) was adopted as it provided a systematic approach for developing the mapping and conducting the analysis. As highlighted in Ackermann and Eden (2004), causal mapping “has a well-established record of use for problem structuring and solution development by operational researchers, both on its own and with other operational research techniques”. The application of causal mapping and analysis has identified the problem of circularity in the principles of information security that are commonly used in existing practice, improve the model developed for addressing the research questions, and helped in understanding the system dynamics of information security systems. These outcomes are described in Chapter 4.

3.3.3.2.3 Four-windows Systemic Analysis

To be better informed about the issues and dilemmas leading to more relevant choices of action for improvement, at the end of each major action research cycle, a systemic approach to interpretation of the analysis was taken in the study. Robert Flood’s (1999)
Four-windows systems view approach was adopted for this systemic appreciation. The “Four-windows” employs four “ideal type” (or categories) to interpret (or view) the data with the intention to stimulate debate, generate insights and enhance learning. The four categories (i.e., windows) are: (1) systems of processes, (2) systems of structure, (3) systems of meaning, and (4) systems of knowledge-power.

As described in Flood,

The prefix “systems of” indicates the desire to be systemic with respect to that category. The four categories help to locate types of issue and dilemma encountered in organizational life. Systems of processes is a category concerned with efficiency and reliability of flows of events and control over flow of events. Systems of structure is a category concerned with effectiveness of functions, their organization, co-ordination and control. Systems of meaning is a category concerned with people’s viewpoints on the meaningfulness to them of what is going on and choices of improvement strategies. Systems of knowledge-power is a category concerned with fairness in terms of entrenched patterns of behavior where what is said to be valid knowledge and proper action, is decided by powerful group (Flood, 1999, p. 95).

While each category provides a different view or interpretation of an action area, resulting in four different impressions of organizational issues and dilemmas, these views are interrelated. Flood asserts that “a holistic, not reductionist, appreciation is sought” which may enrich our systemic appreciation of the complex surrounding, in particular when multiple perspectives of the “Four Windows” are collated and explored.

A summary of the main issues and dilemmas encountered in each action research cycle was also presented in the form of the Four-windows, based on the four perspectives (for example, see Section 4.2.9.)

3.3.3.2.4 Stakeholder Analysis

Stakeholder analysis was used in two ways as part of the study. As part of the Plan-Act-Observe-Reflect action research cycles within the meta-methodology framework of action research, stakeholder analysis was conducted to identify the key stakeholders, the roles of each stakeholder, and how each should be involved in the cycle, in line with the common use of such method as described in Dick (1997d).
In addition, stakeholder analysis was used as part of the research process as a method to analyze the level of supports of key stakeholders in the organization (ALPHA) in the initial reconnaissance phase of the action research cycle, and at the end of action research cycle two following the implementation of the “Model A Approach”. Figure 9, Figure 10, and Figure 23 depict evidence of the outcome of the stakeholder analysis. The results of the two major stakeholder analysis conducted are respectively analyzed and interpreted in Section 4.2.2.1 and 4.3.1.8.

The method of stakeholder analysis as described in Dick (1997d) was adopted. Data generated from the stakeholder analysis were recorded in spreadsheet files and critical reflections conducted over the data are captured in the research journals (for example, J20020617). The list of stakeholders and their roles in the study are described in Section 3.3.1.1.

3.3.3.2.5 Triangulation

A fundamental method applied throughout the study to increase its rigor and improve the validity of its evolving theory was the triangulation of data and critical reflections from multiple sources, using the steps as described in Dick (1996). As described in Section 3.3.3.1, several methods of data collections were applied throughout the study, based on the type and characteristics of the data sources, to enable triangulation to be performed. An example of triangulation was the process of disconfirming the finding in ALPHA that IRM practices in organization was predominantly compliance focused. This finding was triangulated against the outcome of the survey and external interviews as analyzed and interpreted in Section 4.2.

3.3.3.2.6 Negative Case Analysis

Negative cases (Kidder, 1981) identified from critical incidents are sought through the critical reflection and analysis process to rule out rival explanations and fine tune the theory formulated after the fact, at the completion of each action research cycle. In disconfirming the “Model B Approach” in action research cycle 3, which is analyzed and interpreted in Section 4.3.2, negative cases contributed to validating the numerous positive features of the “Model A Approach”, such as its assurance of consistency of practices, cost efficiency, and provides more opportunities for improving IRM competence in different areas of their practices.
3.3.3.3 Implementation Testing

As part of the final action research cycle, the responsive approach was introduced in organization CHARLIE to test its generalizability, and verify its reliability and ecological validity. The test involves verifying the practical use of the information security framework (Appendix D), and the methods supporting the responsive approach, which included the Five Level Actions Map (FLAM, as in Figure 21), and the Dialectic Model of Systems Inquiry, based on Dick’s (2002f) variation of the soft systems methodology and Tay & Lim’s (2004; 2007) implementation.

![dialectic model](image)

**Figure 8: Dialectic model adapted from Dick (2002f) and Tay & Lim (2004; 2007) for organization CHARLIE’s implementation of a responsive security approach**

The implementation, using the dialectic model and the framework for information risk management (FIRM, see Appendix D), consists of four main dialectic processes as shown in Figure 8, as follows:

1. The objective of this dialectic is to understand the problem situation, and clarify the responsive and critical alignment requirements of the business, and related resource (such as people, time, and competence) limitations and constraints (such as regulatory compliance and physical characteristics of building or location) in the organization. The first dialectic involved the following:
   a. Plan, in which I listed the objectives of the project, its desired outcomes, and processes involved and presented to the CIO and CSO for agreement and feedback. I then developed the project plan with the help of the CSO to determine the stakeholders involved and the role(s)
of the individual, in the project and the study. A list of questions was developed using the information security framework to prepare for the interviews in the next step of this dialectic.

b. Act – where I conducted the interviews with the participants, i.e., six staff and the CSO, who described the organization’s environment, including its structure, IT infrastructure, applications, customers, and information involved, in accordance with the components of the information risk management framework. This allowed me to ask questions interactively, and immerse as deeply as possible into the organization to understand the business and its priority. Through the dialectic process, the essence of the organization systems was listed. The IT systems required for supporting the primary priority were examined in further details, identifying relevant risks and limitations in their existing state of operation, including their criticality alignment requirements.

c. Observe – where I listened to the verbal and observed the non-verbal feedback of the participants during the interviews to learn and understand the situation. In addition, I reviewed the available documentations to identify critical incidents while learning about the existing system being practice and the business requirements relevant to information security planning.

d. Reflect – where I performed critical reflection on the information gathered, establishing key risk issues and concerns, responsive and business critical alignment requirements, and looked for disconfirming evidence against them. I also reflected on the outcome against the plan, and the execution of the actions to determine possible improvement for subsequent actions.

2. The purpose of the second dialectic was to conceptualize the ideal information security system for providing the critical functions required by CHARLIE, iterating through the components of the information risk management framework, assuming availability of required resources. The second dialectic involved the following:
a. Plan – The routine function was agreed by the CSO to be out-of-scope for the initial implementation. The CIO identified a suitable IT provider for designing and implementing the new IT systems (to be developed) and scheduled for the second dialectic to take place. I prepared the documents on the essence of the organization systems that were developed from the first dialectic and distributed to all involved for pre-reading.

b. Act – where the two set of participants, one from CHARLIE, as in the first dialectic, and the other from the IT systems design team, an external IT company that was engaged to design the new IT infrastructure by the CIO were gathered for the dialectic session. I facilitated the dialectic session by running through the set of prepared questions and shared knowledge on the information security framework and the responsive approach with the participants. The provider learned the new model and approach, and they in turn contributed by sharing ideas of ideal solutions and approaches for the problems identified in the first dialectic, in line with the responsive and criticality alignment requirements. Majority of the ideal system requirements were dependent on CHARLIE’s new IT infrastructure project. The ideal security systems included all key components of a responsive security system, supported by comprehensive security training and education programs customized for different group of staff to improve their security competency and readiness. After the dialectic session, the IT provider proceeded to design the ideal solution in line with the requirements of the responsive approach and criticality alignment needs of the business. The recommendations were reviewed by the CSO and I before the solution was used as the ideal model. As the CSO desired for the security systems to be certifiable under the ISO/IEC 27001 standard, the information security management system was designed based on the guidelines provided in the standard.

c. Observe – where I observed the proceedings of the dialectic session, including the participants’ comments and understanding of the responsive approach, and how they support the responsive approach
requirements with the available IT solutions. I then reviewed the ideal solution documentation and clarified with the IT provider on specific technical details to ensure its satisfaction of the business criticality alignment requirements (identified in dialectic one), and the responsive security requirements.

d. Reflect – where I reviewed and performed critical reflection on the outcomes of the above steps and the final documentations from the dialectic session for possible improvement in the subsequent dialectic cycle. The critical reflection involved seeking of disconfirming evidence against the completeness of the ideal solution to ensure its validity in meeting the responsive and business critical alignment requirements.

3. In the third dialectic process, the ideal responsive security system was compared with the existing environment and the CIO’s IT infrastructure plan to derive a rationalized system that meets the critical alignment and responsive requirements within the limitation of available resources identified in the first dialectic. The action research cycle involved the following:

   a. Plan – I collated all the documentations derived from the output of the first and second dialectics, established with the CSO the objectives of the third dialectic session, provided required knowledge sharing with the CSO on the process for this dialectic, and scheduled for the conduct of the session. The CSO informed the relevant stakeholders, which involved the CSO team members and the IT provider and prepared them for the session.

   b. Act – The stakeholders gathered and the ideal responsive security system was rationalized against available resources and recognized limitation of the business environment. The final agreed system included a vulnerability management system that provided for swift updating of anti-malicious software programs, and patching of IT systems that were critical to support the new policies requirements. This included a small number of desktop and network systems that were used by the bank’s senior executives, supported by the core
customer database system, and a management infrastructure. A system for improving the redundancy and availability of the core database system was also proposed, since existing system was still on a legacy platform, and would only be upgraded to a new platform when the new IT infrastructure has been implemented, likely in two years period. An incident readiness and response process was also identified through the dialectic session as essential supported by a training program for relevant stakeholders and staff members of CHARLIE. The implementation plan included the selection and assignment of a third party security consulting service provider to conduct an external security penetration test to verify the security of the system against known risks, upon completion. The output of the dialectic was documented and circulated to stakeholders for confirmation before implementation. The CSO was responsible for obtaining the internal budget approval from his senior management for the implementation.

c. Observe – in which I observed the actions of the stakeholders, in terms of their understanding of the process, the responsive approach, and the design of the final IT systems to support the responsive needs and the business critical alignment requirements, and the proceedings of the dialectic session. During which, I took written notes of the participants’ comments, concerns and issues raised and assumptions made. I then reviewed the documentation of the rationalized solution and clarified with the IT provider on specific technical details to ensure its satisfaction of the critical alignment requirements (identified in the previous dialectic sessions), and the responsive security requirements.

d. Reflect – where I reviewed and performed critical reflection on the outcomes of the above steps and the final documentations from the dialectic session for possible improvement in the subsequent dialectic cycle. The critical reflection involved seeking of disconfirming evidence against the completeness of the rationalized solution to ensure its validity in meeting the responsive and business critical alignment requirements.
4. The fourth and final dialectic was conducted after completion of implementation of the final IT system. In the fourth dialectic process, follow-up interviews were held with the CSO and related stakeholders to determine the actual status of implementation of the plan devised from the previous dialectics, again using the information risk management framework to ensure completeness. The objective of this dialectic was to determine if the implementation of the rationalized systems have achieved the desired outcomes identified at the completion of the first dialectic. This involved the following action research steps:

   a. Plan – in which I collated all the documentations that were derived from the output of the earlier three dialectics, established with the CSO the objectives of the four dialectic session, provided required knowledge sharing with the CSO on the process for this dialectic, and scheduled for the conduct of the session. The CSO informed the relevant stakeholders, which involved the CSO team members and the IT provider and prepared them for the session.

   b. Act – the CSO gathered the stakeholders and I facilitated the review of the implementation of the rationalized system, with the IT provider as the main contributor sharing information on the actual status, and outstanding issues to be resolved, including the action plans. The security penetration testing provider’s test plan and report were also reviewed as part of the dialectic. I reviewed the information against the requirements established in the first dialectic, and the rationalized systems agreed through the third dialectic to determine if there were any disconfirming evidence against the claimed status of implementation by the providers.

   c. Observe – in which I observed the proceedings of the dialectic session, and the comments and feedback of the respective stakeholders. At the completion of this dialectic, a new vulnerability management system has been implemented, and the IT systems used by senior executives and supporting staff for the critical policies implementation requirements have been refreshed with the most up-to-date platform and security capability. A security awareness program has also been
implemented, which included training all 2,000 employees of the organization, starting with the senior executives. An external security consultant was engaged to perform security testing on the new systems, which showed that the implementation has been effective against known security attacks, and the vulnerability management system was ready for implementing newer security updates when available.

d. Reflect – where I reviewed the outcome of the actions and performed critical reflection on the observations and analysis to seek disconfirming evidence to determine if the results of the security testing performed by the external security consultant and the state of implementation of the improved systems were as per claimed and presented, and have improved the security readiness of organization CHARLIE.

The outcomes of the critical reflection on the implementation and testing, which showed the validity of the responsive approach, are reported in Section 4.4.7.

3.4 Ethical considerations

Both working colleagues and external practitioners in the same field of practice were recruited for the study. The working colleagues (―internal‖ participants) were from within the same organization and the purpose of their involvement was to validate my personal observations and inferences. The “external” participants were practitioners of information security from other organizations, and they provided the necessary dialectics on the research findings and data interpretation, triangulating towards the final results presented in this thesis. The internal participants were members of a team, of which I was a member, were actively involved in implementation of risk management planning for the organization in which we were employed. The external participants were selected on the basis that (1) they were also involved in managing information security risks in their respective organizations; and (2) they have an interest in learning about new knowledge and practices and how to apply them to their organizations. All internal and external participants were briefed about the research, including the scope of study, purpose, and desired outcomes. All participants were given details about the research and updated on the research findings, progress, observations, and reflections from time to time. Data were collected through the use
of interviews and observations. Journaling was used to log my personal thoughts, including proceedings of interviews, and reflection on observations from the data collected. Dialectics on the actions, progress, observations, and reflections were conducted regularly to triangulate the understanding and chart further courses of action. Participants were also informed that they could withdraw at any time without consequences, although none had exercised this provision.

The main risk to participants (if not managed) was that their identity and the data they have presented might be revealed to others in the organization or in any published documentation associated with the research. Such a risk is only a concern if and only if something adverse or detrimental to the organization or fellow colleagues was discussed and documented. This risk was managed by having all data presented in consolidated manner so that independent contributions would not be identifiable. When a quote was extracted from an interview or a dialogue session with a participant, a pseudo-name for the participant was used. Throughout the study, the participants and organizations’ anonymity was preserved, including any references in this dissertation. I am the only person who knows who was involved in the research and the individual data provided.

3.5 Conclusion

This chapter establishes the criteria for the research methodology, and describes the justifications for the use of action research as the meta-methodology, and also primary research method for this study. The needs for a meta-methodology are also deliberated before the selection of action research as the meta-methodology. The limitations of action research methodology are discussed and addressed through the design and execution of the research procedures.

This chapter also includes an overview of the action research cycles executed in the study, and describes the research process, methods of data collection, analysis, and interpretation used, and the main dialectic procedures involved in the implementation testing of the responsive approach. Convergent interviewing, surveys, observation, critical reflection, learning sets, and validation meetings were employed throughout the study to obtain multiple sources of data for triangulation, increase rigor, and improve validity of the outcome. A variation of grounded theory using data-driven analysis, supported by causal mapping and a systemic analysis technique, was applied
in the data analysis and interpretation processes throughout the action research cycles. The Dialectic Model of Systems Inquiry (DMSI), a variation of the SSM method, was used in the implementation testing procedure.

Chapter 4 describes the outcome of the action research cycles, focusing on the findings established through the data analysis and interpretation of the data collected through the study. Chapter 4 further describes the derived approach, and validation undertaken to gain assurance of its transferability before the study is concluded in Chapter 5.
4 Data Analysis, Interpretations, and Findings

4.1 Introduction

In Chapter 1, I outlined the issues and dilemmas relating to the control-oriented approach in information risk management in organizations in which they were unable to respond to the changing risk environment, which led to the undertaking of this study. In Chapter 2, the literature review established a knowledge gap in current literature in addressing the issues and dilemmas relating to the changing risk environment, including the need for more studies to be conducted in the social-technical aspects of information security. A circular problem was also found to exist in the common principles for managing information security. Findings from the literature review identified the criteria for the desired research approach and provided justification for the use of action research methodology in the conduct of the research, among other methodological criteria evaluated in Chapter 3. The second part of Chapter 3, starting from Section 3.3, further describes the research procedures used in the study, including description of the action research cycles, the stakeholders’ role and involvement in each cycle, the steps taken within the action research plan-act-observe-reflect cyclical steps, and the methods of data collection, analysis, dialectics, and interpretation applied. Through the conduct of the research using action research methodology, as described in Chapter 3, a substantive theory, named as “piezoelectric theory of information security risk management” was developed.

The piezoelectric theory of information security risk management is a primary knowledge contribution to the domain of study. The piezoelectric theory suggests a responsive approach for managing information risk in organizations. The responsive approach is concerned with detecting change events, improving situation awareness, and enabling critical alignment of the organization to respond to emerging security risk situation or incident. The three properties of the responsive approach assimilate the “squeeze-trigger-alignment” attributes of the piezoelectric material, which were validated to be a suitable metaphor and model for improving organization’s readiness to respond to information risk issues and dilemmas, and therefore a primary response to the research questions. The responsive approach also encompasses the need to consider the social behavioral characteristics of organizational risk environments,
incorporating the social-technical approach developed and validated in the earlier phases of the study.

This chapter describes the derivation and development of the piezoelectric approach for information risk management, from the initial metaphor to the validated model, and shows that it is a suitable approach for addressing the issues and dilemmas in managing information risk in a changing risk environment.

This chapter is structured as follows:

1. It begins in Section 4.2 with a discussion of the issues and dilemmas involved in information risk management in practice, including an analysis of their implications to practice and research, based on critical reflection of data and observations that I have completed in action research cycle 1 (“AR1: Understanding the System”, Section 3.3.1), stakeholder analysis of the practice environment in organization ALPHA (Section 3.3.3.2.4), and the mini-survey conducted with external practitioners (Section 3.3.3.1.4).

2. Understanding of the issues and dilemmas further supported the needs to address the social behavioral characteristics of information risk management, and responding to changes in the risk environment, supporting the conclusions drawn from the literature review (Section 2.8). This understanding directed the research towards the development and testing of two social-technical approaches (known as “Model A” and “Model B”, respectively) through action research cycles 2 and 3 (“AR2: Model A Approach”, and “AR3: Model B Approach”, respectively, Section 3.3.1). The outcome of AR2 showed that the social-technical approach (using Model A) was only able to address the research questions partially as it was unable to address unknown and emerging risk issues in the changing risk environment. Through AR3, the Model B Approach was introduced but found to be more problematic, which provided disconfirming evidence for its validity in use in ALPHA for addressing the research questions. These findings are discussed in Section 4.3.

3. The outcomes of AR2 and AR3 also emerged the theme of responsiveness. I therefore directed my efforts in action research cycle 4 (“AR4: Responsive Approach”, Section 3.3.1) to understand the meaning of responsiveness (in sub-cycle 4.1 as shown in Figure 5 and described in Section 3.3.1), and then
design a responsive approach (combining the Model A Approach) and test its validity using case studies conducted in organization BETA, and a series of security and/or catastrophic incidents that occurred during the research cycles, as described in Section 4.4.

4. Through sub-cycle 4.2 in AR4 (Section 3.3.1), the substantive theory was further validated in organization CHARLIE, as described in Section 4.4.7, using the process detailed in Section 3.3.3.3.

5. Outcomes of the validation led to further understanding and refinement of the piezoelectric theory, and the responsive approach for information risk management, as described in Section 4.4.9.

6. The learning and understanding from the study, and the development of the piezoelectric theory, and the responsive approach are further evaluated in Section 4.4.10, which gave rise to the notion of Responsive Learning.

7. Section 4.5 then discusses the responses to each of the research questions listed in Section 1.3.

8. The Chapter closes in Section 4.6 with a summary of the outcomes.

### 4.2 Issues and Dilemmas of Information Risk Management in Practice

One of the research outcomes from this study is a knowledge contribution from the findings relating to the practice of information risk management in the field. Understanding the issues and dilemmas in practice is significant to the development of suitable responses to the research questions, as well as for researchers in future studies in the information risk management knowledge domain. They provide a basis for evaluating the responses to the research questions. Data from the IRM practices in organization ALPHA served as the primary source of data.

#### 4.2.1 Organization and management commitments

To begin, it is important to note that throughout the period of this study, management commitment, in terms of supporting the work of IRM in the organizations where the study was conducted and results evaluated, did not surface as a key issue. The
presence of issues and dilemmas does not signify a lack of understanding by senior management of the importance of information risk management as well. On the contrary, organizations’ demand for addressing information risk issues had been increasing, at least during the period of this research study. For example, in the survey conducted through questionnaires and interviewing of 30 other practicing professionals from the industry (J20061029), the following was established:

1. Information security is now a recognized function in most enterprises, including government organizations, with significant senior management visibility, at a level that is not more than four degrees from the Chief Executive Officer (CEO).

2. The prevalence of information security considerations was supported by 87% of respondents who reported having a security plan in their organizations, and 93% of these respondents based their plan on risk management decisions.

The question was therefore why managing information risk continued to be problematic in organizations, which brought out the importance of understanding the underlying issues and dilemmas involved before attempting to devise and implement suitable responses to the research questions.

4.2.2 A culture of compliance and control-oriented risk management

A common theme that emerged from the study conducted in organization ALPHA, and findings from survey and interviews with external practicing professionals was a culture of compliance and control-oriented risk management approach adopted in most organizations. This was attributed to the nature of the organizational environment, in which regulatory and policy compliance played a significant role in determining the performance of individuals and groups (departments and divisions) in business organization. Information security was part of the regulations and policies requirements, and the status of compliance was the main yardstick used for performance measurement. The objective of information risk management was to ensure that an organization would not get impacted (at least not significantly impacted) due to any information security exposures. In the organizations surveyed and in organization ALPHA, however, information risk management was about managing the risk of non-compliance, to ensure that individuals and groups would not
get impacted due to non-compliance of policy or regulation, but not information security exposures specifically.

In the period of this study, there were five significant incidents (J20020218, J20020611, J20020422-3, J20020401, and J20030818), all resulted in significant impact in organization ALPHA. Information risk managers were unable to play an effective role in responding to those incidents, as individuals and groups in the stakeholders’ departments involved. The incidents revealed the existence of a significant gap between what IRM, individuals, and groups were doing for managing information risk in the organization, and how those activities should help detect and respond to an incident, from the moment a change event emerged to the completion of an incident. In other words, the activities carried out for managing information risks during the non-events period were not helping in either responding or managing the security events that occurred. Changes to the approach to information risk management were therefore necessary and critical to minimize if not eliminate this gap.

The following sub-sections discuss the analysis and interpretation of the empirical data collected and observed that revealed these issues and dilemmas relating to the compliance and control-oriented risk management culture. More importantly, the findings provided an understanding of the plausible development and continuation of such culture and practices, and the responses or approaches necessary for addressing those issues involved.

4.2.2.1 Stakeholders’ support for IRM program

The role and responsibilities of IRM were one that required cross-organization coordination and influencing. As such, IRM required an understanding of the stakeholders involved, and their motivations and goals in their respective areas. I conducted an initial stakeholder analysis (as described in Section 3.3.3.2.4) during Action Research Cycle 1 and identified ten categories of stakeholders. They were: (1) Asia IRM team members; (2) Global Corporate IRM management; (3) Global IRM team members in the line of business outside of Asia; (4) Global Information Security Subject Matter Experts (SME); (5) Technologists in the respective business lines; (6) Business managers in the respective business lines; (7) Operation managers in the respective business lines or locations; (8) General staff members in the
Chapter 4 – Data Analysis, Interpretations, and Findings

technical support function; (9) Senior managers and technologists in the technical support functions; and (10) Members of the senior management team in the Asia Pacific region.

As shown in Figure 9, 14% of the stakeholders were opposed to IRM initiatives, 37% of the stakeholders were indifferent, while 49% were favorable to IRM’s function. In other words, more than half of the stakeholders were assessed in the initial period to be not convinced about the benefits of the IRM initiatives in the organization as they had not seen any positive outcomes from past IRM activities. On the other hand, more than two third of the stakeholders were able to influence IRM’s plans and activities, see Figure 10. The difference in these two charts showed that not all stakeholders were aligned to the objectives of IRM, but their overall influence could negatively affect the outcome of IRM program and activities. Engaging those stakeholders as part of the IRM program was therefore necessary.

![Figure 9: Stakeholder analysis - attitudes of stakeholders towards IRM function](image)

In the 30 organizations surveyed as part of this study, risk decisions in those organization were also found to be based on assessments made by different groups of stakeholders in the organization, including IT auditors (12%), business managers (14%), IT Project manager/team (19%), IT/Operation Risk (24%), and IT security staff (26%). External consultants (2%) played an insignificant role in risk assessments.

In devising and executing its plans and activities, information risk managers therefore need to involve the influencing stakeholders and resolve the alignment issue. Finding common interest between IRM goals and those of the stakeholders would be an important step in achieving stakeholders’ alignment. Although the objectives of information risk management should be common across the organization, individual
goals and agenda often take higher priority, as those were used for individual and groups performance settings and measurements. Information risk managers therefore need to investigate into these individuals and groups’ goals and agenda to identify possible opportunity for alignment.\textsuperscript{75}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure10.png}
\caption{Stakeholder analysis - Capability of stakeholders in influencing IRM Program}
\end{figure}

The views and information provided by each of these categories of stakeholders varied, which further highlighted their individual and group’s concerns, objectives and focus. Actions that were developed and/or performed by groups that were located in Asia usually have a more direct impact on short terms plans and initiatives. The dilemma was that they were often not given equal or higher priority even by the Global IRM function due to different priorities and focus at the corporate level (as discussed in Section 4.2.2.2).

\subsection*{4.2.2.2 Thematic concerns}

As reflected and analyzed in the research logs (J20020312-1, J20020312-2, J20020312-3, J20020316, and J20020318), concerns in information risk management in organization ALPHA centered around five themes evaluated from a number of stakeholders’ perspectives.\textsuperscript{76}

1. IRM staff and managers were concerned about their value contributions to the organization, in which their job security was considered at stake. As a result, IRM staff and managers were focused on activities that could demonstrate
such contributions, giving the main objectives of information risk management secondary priority if necessary.

2. Business management was concerned about poor audit ratings, which were translated as higher Operating Risk Capital\(^77\) (ORC) provisions, meaning more budgets had to be put aside to prepare for the eventual risk exposure, a higher cost of running the business, and a lower profit margin. Information risks were not regarded as high priority action items (as compared to other business priorities), and they were willing to wait for the risks to be managed (J20020312-2). In some business areas, business managers saw risk management as good business practice, but were mostly ignorant of information technology-related risk, and see controls as obstructive to business opportunities. They preferred design-in security protections. A few managers proposed focusing on detection as a means of risk management (J20020316)

3. Auditors saw implementing controls as the means to “managing risk”, i.e., risk mitigation, rejecting other suggestions, such as risk acceptance, transfer, or avoidance measures that might be used. Auditors viewed their job as one to surface as many IT security risk issues to the businesses and IT services and support departments as possible so that they can be addressed promptly. If the business was exposed to the risks, they would be non-compliant with the IT Control Policy, or regulatory requirements. In the latter, the implication could be severe. In the worst case, they could lead to suspension of banking or trading license. However, non-compliant of internal control policies may not have any direct impact to the business. The ORC was therefore designed as one of the elements to address this.

4. Groups that were at the global function level, in New York office, were concerned with consistency of regional processes alignment with global policies and initiatives, such as the global gap remediation\(^78\) project, and their status of implementation. Regional and location-specific initiatives seldom get attention from the global group unless they affect the business’ regulatory compliance status or audit ratings.

5. To the other employees in the organization, risk management and controls meant more work, more procedures to follow, and more hindrances to their
productivity. If a control policy did not affect them, they will reserve their comment or response to it. At times, even if a control policy affects them, they will try to live with it, without understanding what it was for. In other cases, some employees would think of ways to bypass the controls, in a manner that would prevent detection from any external bodies to the department.

It was clear from the analysis that the strongest concerns across all the groups was the audit rating that could ultimately affect the business’ ORC provision directly. Ensuring good audit rating, with a low number of (discoverable) audit issues, and ultimately, low ORC provision in the business therefore was the focal point of the various stakeholders.

As highlighted in Borge (2001, p. 4), “risk management means taking deliberate actions to shift the odds in your favor—increasing the odds of good outcomes and reducing the odds of bad outcomes.” However, in the context of organization ALPHA, to most of the stakeholders, because of the focus on the audit-related metrics, shifting the odds of a poor audit rating became the unwritten primary objective of risk management. Managing risk was about managing compliance to audit’s requirements, i.e., compliance with the IT Control Policy. Risk of non-compliance was clearer than any other risks to the business. This drove a compliance-focused culture based around the IT Control Policy, managing the direct, personal/group-livelihood risk instead of the actual information risk faced by the business.

Evaluating these findings against the work of Argyris and Schon (1991b) and Argyris (2004) revealed that there was a “Theory of Action” at play on information risk management in the organization. In one category, the stakeholders espoused a theory that managing information risk is a practice essential for effective management of information in the organization. However, they demonstrated a “theory-in-use” that was different from their “espoused theory”, in that they were more concerned with good audit ratings, and information risk management was positioned to achieve a good audit rating. In most cases, this theory of action was expressed more subtly, noticeable only by observing their focus and attention in their responses to IRM-raised risks issues versus auditor-raised control issues. When an issue raised by IRM did not get the auditors’ attention, the stakeholders showed little interest in addressing them.
4.2.3 Information risk management practices and implications

As defined in ISO Guide 73 (2001), risk management includes “a set of coordinated activities to direct and control an organization with regard to risk.” As a result of the underlying thematic concerns and “theory-in-use”, the coordinated activities for information risk management practices in the organization were focusing in two areas—facilitation of control self assessment (CSA), and the conduct of “pre-audit” reviews, both to ensure compliance to the organization’s IT Control Policies.

The CSA report formed the basis for the business to understand its risk status, and therefore used as part of the ORC computation. It was also used as an input document to the audit process. Auditors will validate the findings of CSA report to ensure its integrity, and follow-up on control issues that have not been resolved after a certain period of time. As such, this drove the business to either set up a specialized “Risk and Controls” (R&C) function within its department or engage IRM to conduct and validate the CSA process and assessment.

Such a practice (as shown in Figure 11) introduced a number of issues to the information risk management function, and at the same time, created a false sense of security (or controls) in the business.

As IRM and R&C functions were conducting pre-audit reviews, the usefulness of CSA diminishes, since its work duplicated the CSA process. It also indirectly indicated to the business managers that they can take the CSA process less seriously since IRM or R&C was there to make sure that the issue database was updated and validated prior to any audit review.

However, given that most pre-audit reviews were reactive to the audit schedule, the IRM and R&C staff had very limited time to ensure that a comprehensive review was conducted. They therefore focused on what they thought the auditors would look for, normally based on interpreting the scoping document provided by the auditors as part of their entry process. When they guessed the focus area correctly, the auditors would then be unable to discover major issues (since they would have already been resolved or rationalized with justification for their presence before the audit), and the business would get a neutral or positive report. The value contribution of IRM and R&C would be clear and positive in this regard. Nevertheless, the organization will not know the actual information risks and whether those risks had been adequately managed.
The pre-audit approach has its own risk. If the IRM or R&C staff prepared the business to address the issues in an area that the auditor decided not to focus on, or left out a certain area that the auditor decided to evaluate subsequent to the pre-audit review, the outcome of the audit review could be detrimental to the business. The business managers would also question the capability and value of IRM or R&C, resulting in these functions getting penalized for discrepancies found in the business practices. To manage such a “risk”, IRM and R&C staff often ended up as the main coordinator for the business throughout the audit process. This put the IRM and R&C staff in a position that could ensure that the responses to questions and documentation requests from the auditors would answer the auditors’ concerns “appropriately.”

These approaches in dealing with information risk, controls, and audit issues which were still in practice by IRM during the initial action research cycles raised the question about the true value contribution, role and responsibility of IRM, which also related to IRM practices.

Proponents of this approach, which included a number of IRMs, claimed that this was the only way IRM could demonstrate a value contribution to the business. From Argyris’ (2004) “Theory of Action” perspective, this exhibited the defensive reasoning characteristic “to protect and defend the actors”, revealing their practice of a “theory-in-use” that was audit and compliance focused. This theory-in-use “works” when the audit rating was neutral or positive. When the audit rating was poor or negative, IRMs claimed a lack of awareness of the issues involved, and accused the auditor for being out to find problems, and at times blaming the business users for not...
following the rules or procedures involved, either in the system itself, or in “handling” auditors appropriately. Over time, IRM became “skilled in their incompetence” to manage actual information risk, but competent in managing compliance and audit risks. As noted in Argyris, “a consequence of generating skills is designed ignorance”. As such, while in principle, from a domain knowledge perspective, it was clear that such a practice was inappropriate, IRM was either ignorant of or indifferent to such a consequence, since what they had been doing “worked” to justify their existence.

Another reason, according to Argyris’ Theory of Action, was that “organizational defensive behavioral systems encourage cover-up”:

In order for a cover-up to be effective, the intention must also be covered up. It is unlikely that human beings will give or receive useful feedback to deal with their skilled incompetence and skilled unawareness (Argyris, 2004, p. 12).

What this means was that the competence of IRM in identifying and managing information security risk might itself be questionable. By dealing with audit issues and compliance requirements, IRM was not required to identify actual information risks. As long as audit ratings were well maintained (at a neutral or positive level), their lack of information risk management competency would be a non-issue, i.e., covered up.

Since IRM should have a good understanding of the risk issues, businesses felt that they should be in the best position to deal with the auditors, and should ensure that appropriate responses were given to the auditors. From an information risk objective perspective, such a practice was critically inappropriate and unprofessional. It “avoids transparency”, and could be viewed as a form of “self-deception” or “cover-up”, which was another set of characteristics of defensive reasoning. As noted in Argyris, such a mind-set inhibited learning:

The consequences of defensive reasoning include escalating misunderstanding, self-fulfilling prophecies, and self-sealing processes. All these escalate because the logic used is self-referential, which does not encourage the detection and correction of error.

When these conditions are combined, a generic syndrome against learning is created. (Argyris, 2004)
The side-effects on organizational learning and longer term consequences involving the integrity of the business practices in information risk management using the “pre-audit” review practice were potentially detrimental to the organization.

Auditors had rightly expressed deep concerns over such a practice during my interviews with them. Such a practice defeated the purpose of conducting audits, and hindered the auditors in gaining assurance of the integrity of the business system. Ultimately, it blinded the business from the real risks in its environment. In the long run, this could have legal implications.

Even if IRM or R&C was successful in identifying all risk issues prior to every single audit review, the approach was highly reactive, and introduced a fundamental problem from a systemic perspective. As shown in Figure 11, the system was at risk of interruption due to the external events depicted in items (6), (7), and (8). As a result of IRM, R&C, and CSA activities focusing on reacting to audit and compliance needs, with limited time to close control gaps before the audit review, temporary measures were often taken. Root cause information risk issues were often left unidentified and unsolved. Users and managers were not made aware of risk issues and security practices appropriate to prevent and manage them. This indirectly permitted complacency, as depicted in item (6) in Figure 11. When the business environment changes, new projects, technology, and business initiatives, as depicted in items (7) and (8) in Figure 11, they would introduce new security and risk issues, adding to the “systems weaknesses” area in item (5).

Clearly, changes were required in the IRM operating model and practices to resolve these issues, and to address the thematic concerns of the stakeholders. The competency of IRMs also required examination as part of this plan.

The focus on compliance was not a phenomenon that existed only in organization ALPHA. According to Ernst and Young (2005), in their global information security survey conducted in 2005, 81% of the respondents rated “complying with corporate policies” as one of the most important information security functions. To validate this finding, relevant questions were included in a mini-survey that was conducted with the participation of 30 respondents from the industry (J20061029). The survey established that while the main driver for information security was for business continuity, regulatory compliance remained a strong motivator, and the plans and
activities were mostly based on a strategy that was biased towards a defensive approach, which was compliance focused.

IRM needed to achieve its objective of helping the organization manage its information risk. This objective must be understood by all stakeholders. IRM needed to be able to present this objective to the stakeholders to gain their agreement and support. In doing so, it must not result in a compliance and/or control-oriented culture, so that the stakeholders’ focus was on the information risk, and not the status of compliance or controls. The status of compliance provided an indicator of the organization’s control status, but not necessarily its risk status. At the same time, the approach taken must cater to the constantly changing business environment, including IT systems and related risks.

As noted in Hanford (2003, p. 193), “strategic and operational thinking represent very different, albeit complementary, orientations and skills”. The activities that IRM had been performing were mainly operational activities, with attributes such as immediate term, concrete, action/doing, resolution of existing performance problems, and efficiency. To be effective, able to “identity key issues/opportunities, longer term, and reflective/learning”, a strategy was necessary (Hanford, 2003). There was no such notion in the IRM organization. The strategy, plan, and actions taken by IRM, i.e., its practices, needed to change or evolve to address the above needs and challenges.

4.2.4 Risk of Habituation

In organization ALPHA, CSA, as part of the operational risk management system process, was carried out twice a year by the business systems users in the line-of-business (LOB). Business users were to conduct the self-assessment as the ORM group believed that because business users work in the LOB, they would be familiar with the business, and, given sufficient awareness of the business and IT policies, they would be able to discover discrepancies in their practice, or the application systems used, should those practice and systems become problematic. This assumption was questionable.

As noted by Eric Raymond and Rob Landley (2004), “as humans repeat tasks, they form habits—a change that pushes the task from conscious cognition to unconscious cognition”. Habituation, “the process of habituating”, or “the state of being habituated”, is defined in Marriam-Webster as “a decrease in responsiveness upon
repeated exposure to a stimulus” (Merriam-Webster, 2006). When habituation occurs, a person gets used to the stimulus, and loses attention, or becomes indifferent to the event.

Business users, being part of business systems, build expertise by acquiring familiarity with the systems and related processes. In designing business systems, Raymond and Landley emphasize that good interfaces are those that “encourage benevolent habituation” (Raymond & Landley, 2004). As such, over time, users get used to the interfaces, and become proficient in using them with little to no conscious thought. Similarly, if a business application has a security problem, or a vulnerability that was built as part of the systems, eventually, through habituation, users get used to them.

With regards to the CSA process, through habituation, users therefore have a tendency to assess security weaknesses as “normal” conditions rather than exceptions, unless they had recently learned about specific security issues relating to the weaknesses in their system, or had good knowledge of the security policies to discover the weaknesses. The latter was unlikely since users normally would not read the security policies documents, unless they had a recent exposure, such as attendance in training relating to the specific issue just before the self-assessment.

Habituation, as such, presented a risk to the business, in particular, when self-assessment was used as the process to detect risks by the users of the systems themselves. As a result of habituation, users can be blindsided about control issues within their sphere of knowledge and expertise. This provided a plausible explanation for the discrepancies that were discovered by IT auditors in the business areas, when the CSA process had in fact taken place prior to the audit. More importantly, it raised questions on the relevance and usefulness of the CSA process in information risk management. Given that the CSA process was required for regulatory compliance and business governance purposes, whether CSA was a relevant or useful process was, however, out-of-context. To be pragmatic, the IRM Program needed to take additional measures to address the risk of habituation.

IT auditors in organization ALPHA suggested increasing the security risk awareness program, mandating more regular attendance, and building quality assurance checkpoints in the CSA process to ensure the quality of the CSA assessment.
On security awareness, the external survey of 30 practicing professionals (J20061029) further established that:

1. In terms of knowledge and expertise, both at the senior and staff levels, the results showed only slightly more than half of the staff (67%) and security executives (53%) were adequately trained for their respective roles, demonstrating a lack of investment in security and competencies, which were two of the main inhibitors.

2. Security awareness was however regarded as one of the top three priorities in the respondents’ security plans.

4.2.5 Information risk management organization

In addition to the role of IRM, and its value contributions to the business, the organization of IRM and its reporting structure were another area that the key stakeholders showed interest. Two approaches were practiced in the heritage organizations, each having its own merits and issues, i.e., either Business-aligned, reporting to a Head of Business, or Business Operation, or IT-aligned, reporting to the Head of IT Services.

Stakeholders from the business side of the organization (including business IT operation and application development) preferred the business-aligned IRM approach, citing reasons of ownership and accountability of information risk issues (J20020228). Stakeholders from IT Services preferred a centralized IRM organization that would continue to report to the regional Head of IT Services for the Asia Pacific region, citing reasons of: (1) resource efficiency, better cost control, cross-training and learning opportunities for IRM (J20020103); (2) ability to provide an independent view to the business (J20020225); (3) better integration and coordination of IRM activities with IT Services product managers and project managers since they all shared the same end-customers (J20020103); and (3) enabling IRM to disengage from day-to-day business security and risk mitigation operation activities (J20020103). In addition to the issue of organizational alignment and reporting, there were questions about the geographical location of IRM, in particular, whether it should be centrally located or distributed across the region (J20020118). If distributed, what should be the method for determining the distribution? Analyzing the data collected, agreements for a distributed model were focused on ensuring that regional centers had local IRM
managers, since those centers were critical to the businesses and IT operations in the region. A centralized model might incur a much higher cost when IRM needed to travel frequently to different regional centers and branches to execute their tasks locally. Disagreements about a distributed location model were about the cost and availability of competent IRM resources in all the regional centers. They were also concerned about creating location “silos” that would not enable IRM resources to scale up to meet increasing business and IT demands. This, again, would have a cost implication.

The geographical location of the IRM team also raised another concern in terms of location responsibility, including participation in the Location Operating Committee (LOC) meetings, and physical office of the IRM team. Some IRM team members were sitting with the line-of-business, whereas others were centrally located in one office area, together with the IT Services function. Businesses preferred the former arrangement since they can get IRM help easily, but this affected communications among IRM team members, resulting in a lack of information and knowledge sharing, and poor understanding of each others’ work.

4.2.5.1 Systems of knowledge-power

A “Systems of Knowledge-Power” analysis “questions the fairness of designs” with the aim of determining the beneficiaries of the efficiency of processes, and effectiveness of structure in the IRM program. According to Flood, “problematising knowledge-power dynamics deepens appreciation of efficiency and effectiveness and further sensitizes people to the ethical nature of designs and decisions” (Flood, 1999, p. 118).

The question of IRM reporting from the perspective of the fairness of the function in its focus and recommendations versus the reality of the lack of support of the IRM Program by the IT Services group was one of the dilemmas (J20020611). From a management point of view, the use of parallel reporting appeared to be a reasonable solution to the problem. However, the approach to this dilemma was found to be inadequate from a research perspective.

In the business management domain, according to Peter Drucker (1973, p. 517), “organization structure is the oldest and most thoroughly studied area in
management”. This, however, did not seem to be the case in the information security risk management area.

As noted in Chapter 2 (Section 2.5.1), despite the salience of organizational issues, there was little literature discussing the different approaches or organizational models possible, or indicating their importance in the practice environment. Available literature relating to information security risk management—for example, Jackson (1994), Pfleeger (1997), Hansche et al. (2003), Kovacich (2003), and Alberts & Dorofee (2002)—either do not cover or discuss only briefly the organization and reporting structure for an information risk management function. Dorey (1994, pp. 36-39) provides a brief tour of the topic, discoursing on the pros and cons of reporting to the technology function, corporate security, and the Internal Audit department, and highlights the trend towards reporting into the technology function. Parker (1998, pp. 437-473) emphasizes the importance of management commitment, and the establishment and scope of security oversight management committee. The focus of Parker’s discussion, however, like others, is the role and scope of responsibilities, and the tasks (contents of a program) that the function should be performing.

Drucker further states that “organization does not start with structure but with building blocks; that there is no one right or universal design but that each enterprise needs to design around the key activities appropriate to its mission and its strategies” (Drucker, 1973, p. 517). As such, it is reasonable that most researchers and practitioners focus on the activities of information security risk management when discussing the organizational aspects of the discipline.

Despite this, Drucker adds that “the best structure will not guarantee results and performance”.

But the wrong structure is a guarantee of non-performance. All it produces are friction and frustration. The wrong organization puts the spotlight on the wrong issues, aggravates irrelevant disputes, and makes a mountain out of trivia. It accents weaknesses and defects instead of strengths. The right organization structure is thus a prerequisite of performance (Drucker, 1973, p. 519).

As witnessed from this study, the requirement that IRM reporting into the IT Services raised the question of fairness, of whether IRM could still be objective in its work for the business given that it needed the support of IT Services to ensure its welfare and
its performance would be measured by the IT Services functional yardsticks rather than those of the business.

Indeed, the purpose of the structure is to make it possible for each person to “do his thing”.

A hierarchy does not, as the critics allege, make the superior more powerful. On the contrary, the first effect of hierarchical organization is the protection of the subordinate against arbitrary authority from above. A scalar or hierarchical organization does this by defining carefully the sphere within which the subordinate has the authority, the sphere within which the superior cannot interfere. It protects the subordinate by making it possible for him to say, “This is my assigned job.” Protection of the subordinate underlies also the scalar principle’s insistence that a man have only one superior. Otherwise the subordinate is likely to find himself caught between conflicting demands, conflicting commands, and conflicts of interest as well as of loyalty. “Better one bad master than two good ones,” says an old peasant proverb (Drucker, 1973, p. 525).

In discussing the strategy for improvement of systems of knowledge-power, Flood highlights:

There is no short-cut when it comes to knowledge-power. There is no quick fix. There is no instant satisfaction. Yet, engaging in questions [relating to the systems of knowledge-power] … may reveal that improvement simply cannot be reduced to and measured in terms of efficiency and effectiveness. It will not work from anyone’s point of view, whether it is because of unrealized potential in efficiency and effectiveness, or unfair consequences of biased action (Flood, 1999, pp. 121-122).

The findings and assertions of Drucker and Flood, and my reflection on the dilemma concluded, however, that the parallel reporting line to COO-Asia could not resolve the IRM dilemmas. The COO-Asia reporting line risked the creation of conflicting commands from another new authoritative individual, increasing the complexity of managing the relationship with the regional Head of IT Services and the businesses. At the same time, it requires a closer alignment of IRM plan and activities to the COO’s agenda, in addition to those of the IT Services.

Another fairness issue was observed with regard to the notion of a “responsibility axis” as discussed in Drucker.
The organizations of business enterprises and public-service institutions have a number of axes: decision-authority but also information; the logic of the task but also the dynamics of knowledge. The individual jobs have to be designed and positioned in contemplation of a number of axes—task and assignments; decision-responsibility; information and relation (Drucker, 1973, p. 527).

While the “authority axis” was divided into three areas (including one to the global CIRO function), the “responsibility axis” of IRM remained tightly aligned to the global IRM group. As such, on a weekly basis, IRM members were required to participate in international conference calls with their respective global counterparts (Senior IRM) to provide updates of local progress and issues, and at the same time receive information on latest developments in the global arena that might or might not have an impact on local activities. The calls were mostly arranged at New York morning time, which is between 11 and 15 hours later in the Asia Pacific region, depending on specific geography. Consequently, IRM members in the region have to sacrifice family or personal time in the evening regularly to participate in global conference call meetings. Such an issue of fairness was not discussed in the organization, and became an accepted practice throughout (including other functions.)

Reflecting the above analysis suggested that the organization and reporting structure of the IRM organization were as important as any organization in a business enterprise. Besides directly affecting the effectiveness and efficiency of members of the organization, an appropriate structure is also required to promote fairness of practice, or at least enable dismissal of any perceived bias due to a certain line of reporting in the structure. In addition, the fairness of members in the organization in terms of time and resource contribution required to perform their roles are also influenced by the design of their authority and responsibility axes.

While Drucker’s principles for designing suitable structures have been around since the early 1970s, their adoption and practices in the IRM domain have been lacking in organization ALPHA. The principle of systems of knowledge power as used in the analysis of the reflective account of this research sub-cycle further suggested the importance of considering this perspective in the design. Mapping those principles against the issues and dilemmas identified in IRM organization design will therefore serve two basic needs in information security risk management. They are: (1) creating
awareness, and (2) providing useful principles for IRM organization design considerations to avoid related issues and dilemmas in the practice environment.

### 4.2.6 Responding to security incidents

During the initial action research cycle, organization ALPHA encountered two significant but unexpected security incidents. They were: (1) a Simple Network Management Protocol (SNMP) vulnerability incident (CERT/CC, 2002a); and (2) an increase in SPAM email volume impacting the organization’s email services (J20020213, J20020611).

The occurrence of those incidents illustrated a major weakness in the information security risk management program in the organization, as well as the common practices in the industry. In particular, those incidents showed that the focus on compliance and controls did not enable the organization to respond and handle new security issues and related incidents effectively and efficiently. Firstly, the approach and principles adopted by regulators were on addressing known security issues. Secondly, protection, in the form of controls and preventive measures was regarded as more effective for achieving compliance than preparing for the unknowns or unexpected. Finally, the question of dealing with the unknown or uncertain risks was seldom asked and discussed amongst practitioners. Most discussions were focused on technology solutions for the known issues that were most pressing with the auditors and regulators.

In the case of the SNMP vulnerability management incident (J20020213), the immediate issues that were detected were the lack of coordination and an updated database of IT and network systems to allow the state of security of the IT environment to be assessed promptly. The consequence was miscommunication and confusion, as well as uncertainty over who should be responsible for the required data collection efforts. From a control perspective, such discrepancies were also unacceptable.

These issues reflected the state of lack of preparedness and therefore readiness for security events.

The occurrence of these incidents signaled the need for IRM to also consider this aspect, and perhaps incorporate activities in its program to prepare the organization to
respond effectively (J20020218). However, the immediate actions were focused on correcting the “surface defects”, relating to the communication and coordination issues, and the lack of a central IT asset database system.

Those incidents were also not new to the organization. Organization ALPHA, like many others, was impacted by other network worms previously. Experiences from past incidents, such as the “sadmind/IIS” (CERT/CC, 2001a), “Code Red” (CERT/CC, 2001d), and “NIMDA” (CERT/CC, 2001c) worms in 2001 (before the commencement of this study) were not translated into learning and follow-up actions. From an organizational behavioral perspective, this indicated a sign of “learning disability” (Argyris & Schon, 1991b; Senge, 1990, pp. 17-26) across multiple functions, as discussed in Sections 4.3.1.2 and 4.3.3.

4.2.7 Uncertainties in information security risk analysis and management

As reported in Chapter 2, in the knowledge domain, there are issues and dilemmas in the area of risk terminologies, the probabilities of risks, and the methods of risk assessments and management. Collectively, they contribute a cost to risk analysis, and more importantly, uncertainties to the organization. The uncertainties involve in risk analysis are a key issue in risk management.

Figure 12: A graphical representation of common risk analysis and management approach

The common methods of risk analysis and management, such as those detailed in Alberts and Dorofee (2002), Stoneburner et al (2002) and ISO/IEC 13335 standards
(2004; 2005a), may be categorically grouped into four main steps (although some methodologies describe more than four steps.) The first step is to identify threats, vulnerabilities, and exploits that could potentially have a negative impact on the organization’s IT environment, and information. Next, for each of these threats, vulnerabilities, and exploits identified, an assessment is made to determine the probability of occurrence. For each of these threats, vulnerabilities, and exploits identified, in step three, an impact assessment is conducted to determine their potential impacts (or damages) to the organization, normally using three levels of categorization, namely low, medium or high impact.

The results of the first three steps of risk analysis can be plotted in a chart similar to Figure 12. The X-axis represents the probability of occurrence of a threat or a vulnerability being exploited, and the Y-axis represents the potential impacts to the organization if the threat or exploit materialized.

The definition of the three categories along both axes and the boundaries between them are often arbitrary (as observed in organization ALPHA) and subjective, depending on the experiences and knowledge of the risk manager, and the risk appetite of the organization from a policy perspective (as gathered from interviews with the risk managers, and personal experiences). Some organizations define additional categories such as catastrophic, highly critical, and insignificance at both ends of the ease of exploitation, and potential impact axis, to improve clarity of the categorization. In the case of Knowles (2005), the notion of “materiality” was used to signify the criticality of the risk identified and assessed. Figure 12 shows an example of a simple, low, medium and high categorization approach.

The fourth step is then the risk management recommendations, on how each risk item that has been categorized should be managed. From this assessment, with the chart plotted, it is clear to the risk manager and also senior management that the top right hand corner areas of the chart should be the focused area for actions and resources allocated in order to gain the highest returns of investment in risk management.

When additional resources are available, the medium categories are the next in line for actions. They are also considered when the cost of actions is assessed by the risk manager as low or affordable. In most information risk literatures, this is denoted as a curve as shown in the shaded area in Figure 12.
As for the low risk/impact categories, they are often justifiably left out from the action plan, or information security risk management program, since they are assessed to have a low probability of occurrence, and/or low impact to the organization.

With the above assessment, the common strategy for the information security risk manager is to drive the curve towards the left as much as possible, so that more risk issues get addressed. This was a strategy adopted in organization BETA, as shown in Figure 13. As also shown in Figure 13, the lower risk areas are denoted as “acceptable risk” to the organization.

But this strategy alone may increase the cost of security. As highlighted by Knowles (2005), in terms of actual implementation, an optimal spending on security needs to be justified, since it is an area considered as a cost to the business. In this regard, approximation chart such as Figure 14 is commonly used to map the cost of implementing security against the potential business impact to derive the optimal focus required.

As realized from the analysis conducted in this study, this approach of risk management has several limitations in ensuring information security in the organization. A significant issue relates to the capability of the organization in responding to new risks, errors in risk assessments, and other security events and catastrophes, as discussed in Section 4.2.6.
As Peter Drucker commented on management’s fear of risk-taking:

What is lacking in the management sciences as applied today is the emphasis throughout its literature and throughout its work on “minimizing risk” or even on “eliminating risk” as the goal and ultimate purpose of its work.

To try to eliminate risk in business enterprise is futile. Risk is inherent in the commitment of present resources to future expectations. Indeed, economic progress can be defined as the ability to take greater risks. The attempt to eliminate risks, even the attempt to minimize them, can only make them irrational and unbearable. It can only result in that greatest risk of all: rigidity (Drucker, 1990, pp. 511-512).

In analyzing the security incidents (Section 4.2.6), from a systems perspective, organization needs to go beyond just risk mitigation. The inability of the organization to respond was established as a key factor that prevented the organization from addressing the emerging events appropriately. This further suggested possible discrepancies between the action strategies in existing IRM practices and the processes used in addressing new or emerging risks. One of the discrepancies can be traced to the limitations of the risk analysis and management approach that is commonly adopted in organizations (like in organization ALPHA.)

Firstly, on risk identification and categorization, the assessment was subjective, highly dependent on the experiences of the risk manager concerned. As reviewed in Section 2.3.6, there was no reliable method for quantifying information security risk. Risk assessments were therefore qualitative. When quantitative methods were used, the numeric assignment of risk level falls back to a qualitative assessment. The use of
probability was therefore prevalent, but has its unique issues (as discussed in Section 2.3.6). A low risk item assessed by a risk manager therefore may not necessarily be assessed as low risk by another.

As highlighted in Kabay (2002), the perception of security and risk varies between individuals. To some risk managers, when a security weakness in the system is identified, and an attack is assessed to be easy to execute, the probability of occurrence is deemed as high. If the attack is assessed to be difficult to execute, the probability of occurrence would normally be assessed as low. This assertion, if true, however, can only be partially true, since not all difficult-to-exploit vulnerability will necessarily have a low probability of occurrence. An exploit might be assessed as “difficult” to execute by a risk manager due to her capability and experience, but to a perpetrator, she might have already developed the tools required to ease the attack. The problem is highly asymmetric. The risk manager has to know a lot about the systems under assessment, but still does not know what the perpetrator knows. The perpetrator only needs to find a security weakness that she can exploit.

Learning from the insurance business, in most risk assessment, risk managers based their assessments on a priori of occurrence as a primary indicator of the probability of occurrence. Experiences influence individuals’ perception cognitively. As noted in Elizabeth Styles, prior exposures contribute to the experiences.

The processes involved in visual perception enable us to act and react to the visual environment safely and accurately. We need to know what things are and where things are, and where we are in relation to them…

Together with attentional and memory processes, perceptual processing gives rise to our experience of the visual objects and events around us (Styles, 2005, p. 49).

John Adams (1995, pp. 14-15) also postulates that “perceptions of risk are influenced by experience of accidental losses—one’s own and others”. Experiences of past incidents therefore contribute significantly to a risk manager’s assessment. However, there are often many factors that contribute to the occurrence of an accident. Besides bad practices, as Adams highlighted, accident may also result from individuals’ risk taking behaviors (1995, pp. 52-55). A risk event that has occurred previously provides data to show the possibility of the risk event. Actions of the risk managers, and changes in the organization might have brought a closure to the exposures relating to the risk event, or make it more vulnerable. On the other hand, the non-occurrence of a
risk event does not signify a low probability for its occurrence in the future. When there is no prior incident or precedence to rely upon for assessment, imaginations and creativity of individual risk manager will play an important part in the assessment, mostly tapping on her knowledge and past experiences. As Posner (2004, p. 171) commented in his discussion on the risk associating with the September 11 incident in 2001, “it would be a mistake to dismiss a risk merely because it cannot be quantified and therefore may be small—for it may be great instead.” In the aftermath of the Hurricane Katrina (CBC, 2005; CNN, 2005) disaster in New Orlean, Ronald J. Daniels, Donald F. Kettl, and Howard Kunreuther asserted that:

> It is not easy to assess low-probability events and people often disregard them. There is ample evidence that people often do not want to consider data on the likelihood that an event might occur, even when the information is available to them. Only after a disaster do most people pay attention to it, and then they overestimate its likelihood (Daniels, Kettl, & Kunreuther, 2006, pp. 6-7).

The final assessment of the risk manager is therefore subjective, depending on her beliefs, shaped by her risk perception, and how she influences other stakeholders to her perspective. As such, low risk areas that are charted out below the curve in Figure 13 may turn out to be erroneously assessed, but high risk in reality. Similarly, a high risk item may be identified simply due to a rare prior occurrence.

From the cost management perspective, as highlighted in Knowles’ “optimal cost” approach, low risk issues, and to some extent, depending on budgetary, medium risk issues are unlikely to get any management attention. However, due to the asymmetric nature of the problem, they would likely be what the perpetrators targets. This results in a risk management paradox.

In addition to errors and perceptions contributing to the subjectivity of a risk assessment, there are other unknowns (that may be known only to the potential perpetrator, but not to the risk manager) that can influence the risk situation of the organization.

One example is undisclosed vulnerabilities that are known only to the perpetrator, but kept secret for various reasons. A perpetrator may have economic benefits in exploiting vulnerabilities. As reported in the Business Week, skilled hackers were on the payroll of businesses for competitive reasons (Blank, 2001). In addition, according
to Techdirt.com (2006), “malware\textsuperscript{97} writers are more likely to be in the virus writing business these days more for profit, rather than fame or for kicks.”

That also means that the type of malware being written is changing as well. Rather than go for the big hit, with a virus that spreads super fast and makes the headlines, virus writers know that they're better off being sneaky. The less well known their viruses are, the less likely they are to be stopped by security software... and the longer there is to profit from the malware (Anonymous, 2006).

Undisclosed vulnerabilities will therefore continue be one of the unknowns to the risk managers, even though they could be known to the perpetrators. Some of those vulnerabilities may also be known to the technology provider, based on their internal research, or reports received from other researchers without disclosing their findings publicly. In organization BETA, which is a technology provider, I further learned that technology provider could not share such publicly unknown vulnerability information with the end-user organizations, as doing so may inadvertently disclose the information to potential perpetrators who could then use the information to their advantage. Furthermore, when a security weakness has not been fixed, releasing the vulnerability information without providing a fix could result in undue panic in the end-user organizations. Most technology providers therefore promote the principles of “responsible disclosure”\textsuperscript{98} to strictly limit sharing of the vulnerability information only with responsible parties until such time when a fix has been completed.

Even if the risk manager is able to identify and quantify all the risk dependencies, the outcome of the risk assessment (as shown in Figure 12) provides only a snapshot of the situation that the organization is challenged with. The operating environment, both inside and outside of the organization, is a constantly changing environment. Each change can have neutral, negative, or positive influences to the risk status of each risk item involved, and the systems as a whole. Changes may be planned, as in the case of implementing a new information systems to support a new business application, or unplanned, as in the case of the SNMP vulnerability, SPAM, SQL Slammer and Blaster worms attacks, the SARS epidemic, and the Tsunami tragedy. Risk may be identified and managed as part of the planned change, but often only becomes visible after an unplanned change. This means that risk related information that can be learned from personal experiences and information sources are limited. The risk
manager’s assessment of risks would therefore have to be discounted from the unknowns.

As Charles Perrow (1999) observed, the characteristics of complex systems are such that the effects of failure in one component would often result in unpredictable changes and consequently, failure to other components leading to eventual failure of the system as a whole. Technology systems that are interactive and/or tightly coupled are most prone to such failure, which Perrow named as “normal accident”, or “systems accident” (Perrow, 1999). Perrow therefore concluded that “no matter how effective conventional safety devices are, there is a form of accident that is inevitable.”

As also observed by other practitioners, like Venables (2004) and Mahtani (2004), and researchers, like Blakley, et al. (2001), the information security risk environment is highly complex, not all information security risks can be identified or predicted accurately. As in any complex systems, the element of uncertainty prevails.

The potential for errors, perceptions, and uncertainties involved in risk assessment are the key limitations to the common method and strategy for managing information security risks in organizations. Collectively, and individually, they contributed to the losses and negative consequences from the numerous security incidents and natural disasters.

Most organizations, like in ALPHA, address the uncertain risk issues as part of the disaster recovery or business continuity management, as part of the X-Y axis view, denoting them as part of the high-impact low-probability risks to the organization. This leaves significant gaps between risk management and incident recovery. Risk managers were therefore often caught off-guard when seemingly low risk issues were exploited to cause massive disruption to the business (as in the case of the SQL Slammer and Blaster worms incidents.)

4.2.8 A Causal Analysis of Information Security Systems

Causal analysis provides another means to understand the systemic issues in a given environment or system. Figure 15 depicts a causal view of the information security systems. This empirical view may not be the most complete, but captures the essence of the information security system and the related attributes that are sufficient for the
purpose of this discussion. Details of the causal analysis I have completed was reported in Kang (2005c).

As analyzed in Kang (2005c), if the information security system is left on its own to operate in response to external events and developments, over time, there will be inadequate resource investment to sustain the pro-active initiatives and programs required to reduce or eliminate undesirable behavior and activities in the system. Instead of waiting for more losses and damage to trigger an increase in resource investment for ECDR and LEPE, proactive steps are necessary to sustain investments in order to keep the system balanced with the positive (solid-blue) outcome cycle running instead of the negative (dotted-red) outcome cycle. Lower or no LD will result in sustaining, if not increasing, the business value of IT, since the information systems are secured and protected, and able to address business needs at an optimum level of performance, quality, and reliability. By keeping a healthy level of RI for ECDR and LEPE, the information security system will therefore operate in a balanced condition whereby the risks of attacks will be managed (Kang, 2005c).

While realizing the existence of this causal system is important, its awareness alone is insufficient to drive information risk management requirements into the stakeholders’ immediate agenda. Organizations need a more strategic approach to bring the alignment so that a healthy level of resources is provided to maintain the ECDR and LEPE related activities.
4.2.9 Summary of issues and dilemmas

<table>
<thead>
<tr>
<th>Systems of Process (Efficiency &amp; Reliability)</th>
<th>Systems of Structure (Effectiveness)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes (in the form of pre-audit reviews) designed in response to audit and compliance issues, based on IT Control Policies, not based on sound information security or risk management principles; Unable to detect emerging risk issues; Unable to respond to changes in the risk environment, including critical security events and resulting incidents.</td>
<td>Issues involving IRM organization structure, roles and responsibilities, funding arrangement, and physical location. Fragmented structure, some IRM staff members continue to report to business IT/Operations, others taking instructions directly from IT Services; Geographical (location) requirements not met consistently; Confusion of IRM roles and responsibilities, and value contributions; Poor communication within IRM group, little learning and sharing of knowledge.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Systems of Meaning (Meaningfulness)</th>
<th>Systems of Knowledge-Power (Fairness)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of clarity of authority and ownership of information risk issues; IRM pressurized by multi-stakeholders to focus on compliance in order to demonstrate value contribution; Reactive to audit and compliance issues; Little learning for IRM members in information risk domain; Concerns over job security (by IRM members) influence IRM activities towards need of business managers to improve compliance rather than managing information risk.</td>
<td>Governing ideas influenced by auditors, business functions, and global senior management, but not IRM. Actions taken in IRM were issues driven, and fall into the flow of the causal system if left unmanaged (as shown in Section 4.2.8).</td>
</tr>
</tbody>
</table>

**Table 1: Four Windows (Flood, 1999) systemic view of information risk management situation in organization ALPHA during action research cycle 1**

The issues and dilemmas involved in information risk management practices, learning from the practices of organization ALPHA, and the other 30 practicing professionals,
may be summarized using the construct of Robert Flood’s Four-windows systems view as depicted in Table 1.

The findings re-affirmed the issues in information risk management that were identified in the current literature, as described in Chapter 2, and further established the dilemmas involved, such as the presence of multiple stakeholders, implications of non-compliance to regulatory and internal IT Control Policies, and the lack of competence in IRM and various stakeholders in the knowledge domain. These findings revealed two main threads of inadequacies in the current model of information risk management being practiced.

One is the lack of consideration on the systemic aspects of the individuals, and groups involved in the information security system, basing actions on compliance needs and reacting to incidents without adequate preparation and readiness. Another is the lack of consideration of the underlying assumptions and potential errors of current risk assessment methodology applied, i.e., the need to cater for the unidentified or errors in the risk assessment, and the need to cater for change in the business, technology, and overall risk environment.

In response to the research questions and these findings from the initial action research cycles and related literature reviews, the research design was revised to approach the research problem by developing and testing two approaches focusing on these two aspects of findings.

The first approach entailed the development and testing of a social-technical model, involving two organizational structures in response to the issues and dilemmas identified in the organizational aspects above, focusing on the “soft” issues identified.

The second approach focused on the notion of responding to changes in the risk environment. The piezoelectric principle surfaced during this process and was subsequently adopted as the metaphor and model for developing and testing this approach.

Sections 4.3 and 4.4 describe and discuss the two approaches undertaken in the research study, including the outcomes of the testing completed, and the main findings from the analysis, interpretation, and understanding obtained.
4.3 A Social-Technical Approach

The social-technical approach introduced changes to the IRM system and practices by adopting social science and systems thinking techniques in understanding individuals and organizational behaviors and devising plans and action strategies that address key attributes identified from the knowledge acquired. Two sub-models, known as “Model A” and “Model B”, respectively, were implemented in three action research cycles to test the efficacy and suitability of the changes in addressing the issues and dilemmas discussed earlier. The “Model A” Approach set a new structure, operating model, and a comprehensive program, evolving from the current practices, incorporating the social-technical elements necessary to address the concerns. “Model B” Approach differs from “Model A” in the organization structure and operating model, while maintaining the design of the IRM Program. “Model B” was an incidental model, forced upon the study as a result of the changes in the organization itself. This was inevitable, and a known side-effect of action research methodology whereby the workplace is used as part of the research environment.

In both approaches, IRM issues and dilemmas highlighted in the earlier Sections formed the basis for the design and testing of the models developed. This included addressing the “theory-of-action” issues identified among the stakeholders.

4.3.1 Model A Approach

The “Model A Approach” for managing information security risk in organization ALPHA was implemented and tested in two action research sub-cycles, namely, “Do something differently”, and “Solve the problems”, outlined in Section 3.3.1 (and also detailed in J20060819). The iterative nature of action research was used to incrementally improve the approach devised. The technical aspect of the model included three main components:

1. An IRM organization structure with a centralized resource model cost funded by the various lines-of-businesses, including IT Services;
2. An IRM operating model providing clarity on roles and responsibilities (J20021217);
3. An IRM Program, incorporating:
a. A sub-system for identifying critical business and IT systems for ongoing risk reviews;

b. A sub-system to conduct risk reviews on business applications and IT infrastructure systems;

c. A scorecard-supported system for performance measurements and management reporting;

d. A series of remedial action programs, devised and implemented with the respective stakeholders and issue owners;

e. An improved information risk awareness program, with more extensive tracking of participation, and focused topics for addressing the awareness needs of staff in different stakeholder groups;

f. A learning-set for information risk managers to learn and practice an action learning-based inquiry into their practice, and share their learning experiences.

The social aspect was the focus on individuals and group from a systems thinking perspective, using social science techniques in improving understanding of their needs and motivations, and influencing their acceptance and consequently, actions in line with the objectives of IRM and IRM Program.

The learning, analysis and interpretation through the implementation of the “Model A Approach” resulted in the formulation of a “five-level action strategies” model as shown in Figure 21, and a social science techniques enhanced IRM system, known as the SECD4 system model, as shown in Figure 22.

4.3.1.1 Addressing the IRM and business/IT managers’ theory of actions

From a systems thinking perspective, the theory-in-use of IRM members, and business/IT managers reflected a “Shifting the burden” system archetype structure (Senge, 1990). As shown in Figure 16, the normal practice environment in business and in IT operations were risk controlled through standards established in the organization’s IT Control Policies and Standards. The business users and IT systems were required to implement and practice those controls.
Security weaknesses in the business and IT systems were not, however, detected immediately, as indicated by the “delay” element in Figure 16. The Control Self-Assessments (CSA) process was established as a measure to detect systems weaknesses and develop action plans for their resolution. This, in the theory espoused by the operational risk managers, would improve the systems practices and behavior resulting in a better risk-managed environment.

As indicated in Figure 17, the integrity of this system was periodically tested by the auditor, as an independent third party. When inadequate practices or security issues were detected, the business involved would receive a poor audit rating, and be subsequently penalized with an increase in their operational risk capital. This often resulted in pay freezes, cost cutting, and/or dismissal of staff involved in the security problems. As such, business and IT managers were prompted to respond.

The theory-in-use, of conducting pre-audit reviews, was a symptomatic response to the audit challenges. As shown in Figure 18, together with the introduction of new (mostly reactive) controls, and the escalated use of the Risk Acceptance process, a balancing loop to the audit review was created. No action was introduced to
Chapter 4 – Data Analysis, Interpretations, and Findings

strengthen the fundamental response to balance the audit review loop. The side-effect of this was not clear until the structure was re-drawn in Figure 19.

![Diagram of audit review loop with risk acceptance and IT control policies]

**Figure 18: Symptomatic response to audit interventions**

The pre-audit review and risk acceptance activities formed a “shifting the burden” structure described in Senge (1990, pp. 104-113). The longer term implication of this structure was an increase in complacency, and a degradation of the IT control policies, as noted in Figure 19. This was evidenced by the numerous audit issues that were detected by the auditors and found to be caused by human complacency, not following the established procedures, and missing of crucial steps in executing a control procedure.

![Diagram of “Shifting the burden” structure with symptomatic response]

**Figure 19: “Shifting the burden” structure enforced with symptomatic response**

Using risk acceptance as a process, numerous difficult controls to implement or were comply with were “risk accepted”, and therefore not practiced. Through pre-audit review, business and IT users waited for the reviews to identify issues, and addressed them only in time to meet the auditor’s review schedule. When the audit review was over, their previous practices resumed. This was evidenced by the many findings of repeated issues in the review reports.
In order to make positive changes to systems, Senge suggests the “principle of leverage—seeing where actions and changes in structures can lead to significant, enduring improvements.”

Often, leverage follows the principle of economy of means: where the best results come not from large-scale efforts but from small, well-focused actions. Our non-systemic ways of thinking are so damaging specifically because they consistently lead us to focus on low-leverage changes: we focus on symptoms where the stress is greatest. We repair or ameliorate the symptoms. But such efforts only make matters better in the short run, at best, and worse in the long run (Senge, 1990, p. 114).

From a systems thinking viewpoint, the IRM program reinforces the actions as a fundamental response to the audit challenges by introducing two key processes to the system—increasing awareness of risks, and conduct of ongoing risk reviews—as depicted in Figure 20.

![Figure 20: Enforcing fundamental response by IRM Program](image)

The analysis therefore showed that the IRM program was systemically sound, and the results enabled further understanding of the differences between the new program and the previous practices.103

**4.3.1.2 Addressing the Auditors’ Theory of Actions**

The theory of actions practiced by the auditors was observed from their interpretation of the meaning of information risk management. In line with most practitioners’ expressed view of “no perfect security”, they agreed that a risk-based approach to managing information security risks was necessary. However, when a security issue was identified, in which no solution using available tools or procedures could be found,104 and the resolution required a risk-based decision to be made, the auditors were often reluctant to accept it. This was exhibited in numerous occasions in their
imposition of a lengthy process and strict criteria for the risk to be accepted, and the strong enforcement of “compensating controls” using extensive manual procedures that were inefficient and ineffective.

Reflecting on the philosophical perspective of Soft Systems Methodology, citing Checkland (1983), Michael C. Jackson highlights the “hard” systems paradigms:

Hard approaches assume the world contains systems the performance of which can be optimized by following systematic procedures. These procedures involve establishing clear objectives and then using generalizable models, based on systems logic, to enable prediction and control of the real-world systems of concern so that the objectives are realized with maximum efficiency and efficacy. Unfortunately for hard systems thinking, logic is usually much less significant in terms of what happens in organizations than is the history, culture and politics of the situation (M. C. Jackson, 2003, p. 185).

In contrast, as noted in Checkland and Howell (1998, p. 71), the soft systems paradigms “advocate taking a more tribal view of organizations, and adopting a more interpretive approach to inquiry.”

An organization is to be seen at core as a social process, essentially a conversational process, in which the world is interpreted in a particular way which legitimates shared actions and establishes shared norms and standards (Checkland & Holwell, 1998, p. 71).

The auditors’ theory-in-use of seeking out mitigating measures rigorously regardless of the actual risks involved further suggested that they viewed information security as a “hard” problem, i.e., the view that if there is a process that people follow, then there is a solution to the problem. Therefore, if there is no technical solution, then there must be a procedural solution to either compensate for it or resolve it. The “soft” aspect of the problem was disregarded. This contradicts my proposition that information security is a “soft” problem as concluded from the synthesis of literature reviewed in Section 2.7 in Chapter 2. There are several possible reasons for this contradiction:

- The organization’s systems, in general, were based on the classical approach that is predominantly a hard systems paradigm. As such, citing March and Simon (1958), Checkland and Howell (1998, p. 45) highlight that people in such organizations will follow the practice of seeing “‘problems’ as ‘indicated
by gaps between performance and goals’ and ‘problem solving’ is then a matter of closing the gap by finding a suitable means to achieve the goal, which is taken as already known”;

- Lack of awareness or appreciation of the concepts of “hard” versus “soft” sides of information risk problems; and

- “Soft” issues are social issues, which often require social trust before problem resolution. In this context, it required the auditors to trust the business users and IT staff to comply with established policies and procedures in their practices. This was fundamentally against the nature of their role, which was to validate that the practices were adequate.

As noted in Fukuyama (1995), the extent to which a person or group will trust another is also cultural bias. In an organization with a diversity of people from different cultural backgrounds and upbringing, trusting people to address risk issues can be viewed as a challenge. It could be a behavior that auditors could easily assume, especially when they are not part of the business department being audited, and do not share many cultural norms with the individuals and groups involved.

Fukuyama further adds that, “trust is the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of other members of that community” (Fukuyama, 1995, p. 26). A business organization, in essence, can be viewed as a community with a common interest (of achieving the business objectives), with a range of commonly shared norms. For example, believing in the company’s vision and mission statements, and practicing the defined core values. In this regard, from a theoretical perspective, based on the assumptions that those core values, common vision and mission can become established norms, and the organization has the ability to recruit honest people, the notion of trust is not entirely out of reach within a business organization. Nevertheless, the extent to which this can be achieved in each organization is subjective. The results are also often unpredictable as the many external and internal changes and relationships between individuals, individual and group, and individuals and the organization are highly complex.

While building trust among individuals and groups within an organization may improve business efficiency and information security practices by raising individual
commitment, such an approach was found to be unacceptable by the regulators. As noted in the study (J20020208), in a meeting held with a senior executive of a regulatory body, one of the biggest concerns of the regulator was insider threats:

Insider threats are the biggest threats to financial institutions. If an insider can gain access to customers’ sensitive information, and use them illegally from the outside, they could cause massive damage to the institution. In addition, this could also affect the economy and confidence of the financial market in the country (J20020208).

From a risk perspective, what the regulator had highlighted was actually its concern over the impact and consequences of an attack. There are other attacks that may result in similar outcomes that the organizations tried to protect against. As long as the attacker is able to find a weakness to exploit, she can achieve her desired outcome regardless of whether she is an insider or outsider. The risk of such an outcome needs to be assessed from a number of angles and constituents of risk itself. The nature or profile of the attacker is merely one of the many facets of this assessment. Other factors, such as the normal operating conditions of the systems involved, the protection accorded, the rigor of monitoring exercised, and the effectiveness of the response systems all play a part in preventing, detecting, and minimizing the attack and damages.

There is also no guarantee that in a fully controlled environment, no insider attack will be possible. As shown in Mitnick, et al. (2005; 2002), humans can and often do fall prey to social engineering attacks, and outside attacks have been increasing due to the proliferation of networks and systems connectivity. Similarly, it has not been proven that a high trust society will necessarily result in more insider crimes. On the contrary, Fukuyama (1995, p. 310) found that “the decline of social trust is evident on both sides of the law, in both the rise of crime and civil litigation”.

The decline of trust and sociability in the United States is also evident in any number of changes in American society: the rise of violent crime and civil litigation; the breakdown of family structure; the decline of a wide range of intermediate social structures like neighborhoods, churches, unions, clubs, and charities; and the general sense among Americans of a lack of shared values and community with those around them (Fukuyama, 1995, pp. 10-11).

Taking action to improve social trust in the organization is therefore an important step to reduce security breaches and minimize the possible realization of information risks.
from inside the organization. Incorporating social science and systems thinking techniques in the IRM program is therefore essential to this objective of improving social trust between the stakeholders and IRM in order to improve management of information risk in the organization.

The theory of action in which the theory-in-use differed from the espoused theory in these two groups of stakeholders further supported the inference that there was possibly a “learning disability” (Argyris & Schon, 1991b; Senge, 1990, pp. 17-26) problem in the organization, including IRM staff members, as identified earlier in Section 4.2.6. The IRM Program, which placed focus on improving social interaction, involved ongoing dialogues with the auditors, which therefore helped to improve their awareness and appreciation of the “soft” side of information security risk.

4.3.1.3 Competency and Trust

The issue of competency resurfaced during this phase of the study (J20030425). There were two aspects of competency that needed attention. They were the competency of IRM, which was addressed in the action strategy directly, and the competency of the staff members of the stakeholders’ functional areas.

As reflected in J20030705, learning from Peter J. Denning, competency is important from a trust perspective:

> Trust is an important assessment we make about others and others make about us. If others trust us, we will accomplish much. If others distrust us, we will accomplish little (P. J. Denning, 2003).

How do I build trust between IRM and the staff members of the lines-of-business and IT Services? This was an issue that was also found in the second action research cycle, in which the data analysis (J20060819) concluded that taking action to improve social trust in the organization was an important step to reduce security breaches and to minimize the possible realization of information risks from inside the organization. To establish and build trust, Denning suggests taking a language-action perspective to interpret trust:

> Trust is an assessment of confidence that an outcome will actually be accomplished and simultaneously an acceptance of the risk that it will not be. Trust is an emotional skill in which we align our intentions and our sensations of readiness for action (P. J. Denning, 2003).
 Appealing to the emotional element of trust appeared to be a possible approach to obtain commitment and to stimulate more positive action from the stakeholders and related staff members. This should include clarifying the consequences of their inaction or poorly executed actions that could affect the information risk of the organization, besides just poor audit ratings, which was often their only concern. This approach, however, requires IRM members to communicate with the stakeholders on a one-on-one basis, at a more personal level, when working with the individuals involved to review and resolve security risk issues in their respective areas in the line-of-business and in IT Services. According to Denning,

> Our trust in someone’s promise is based on sub-assessments of competence, sincerity, and capacity. Competence means the person has the embodied skill to deliver what he promises. Sincerity means the person’s private and expressed intentions are the same. Capacity means the person has the time, resources, and favorable circumstances to succeed. We won’t trust someone whom we think is incompetent, insincere, or lacks capacity. We won’t trust someone who breaks promises. Simply knowing this can help us shape our actions so that we are seen as trustworthy (P. J. Denning, 2003).

This view therefore relates back to the competency of the IRM members, which is a critical element in gaining trust and commitment from the stakeholders’ staff members. Denning states that:

> The term “embodiment” refers to knowledge “in the body”, ready for immediate performance when the situation arises. This form of knowledge is distinct from conceptual knowledge, which is “in the mind”, ready to provide explanation or description. An embodied capability includes a well-honed set of interpretations of the world, allowing the expert to immediately “see” what is needed in a situation and to act on it without thought.

To many, the notion of putting the body into learning is unfamiliar. Most technologies rely on difficult intellectual abstractions. Mastering them appears to be the key to advanced education.

In real life, we instinctively understand the difference between conceptual knowledge and embodied knowledge. We will choose the dentist who has crowned 100 teeth, the surgeon who has performed 1,000 procedures, or the pilot who has flown 10,000 flights (P. J. Denning, 2002).
Similarly, we will chose information risk managers who have risk-assessed different types of information systems in different contexts, and who have real life experience in managing a firewall network or have performed security administrations before in a nearly similar environment. But IRM needed time to gain the experience and acquire the embodied knowledge. Similarly, staff members of the lines-of-business also needed time and practice to be risk-aware, and to manage risk in their respective areas. A common practice, as also adopted in organization ALPHA, was to define the competency needs as a standard in the individual IRM staff member’s job description.

As noted by Stewart Hase and Boon-Hou Tay, “standards have had a profound effect on how we consider issues of quality, selection, promotion, performance evaluation, training, and project management.” Despite this,

Standards seem to suggest linear thinking about performance. If a person, group, or organization can achieve a level of performance once, then it can do it again. That somehow the environment in which this happens is as predictable as the outcome (Stewart Hase & Tay, 2004).

As experienced in the research cycles conducted since the beginning of this study, the organizational environment in which IRM staff operates is essentially complex.

Given the propositions of complexity theory, developing competency is a minimum standard for dealing with rational, linear systems. But, we need capable people to deal with the unpredictable nature of complex environments. We also need to consider how to develop work environments that enable capable people to express their capability (Stewart Hase & Tay, 2004).

A standards-based approach to establishing and building competency will therefore deliver limited capabilities to the IRM members and their constituents.

What we are interested in is how to go beyond this baseline to capability, the preparedness for applying standards and using competence in novel, complex situations rather than the familiar.

We suggest that the emphasis needs to be in the organizational processes that are used rather than the outcomes.

The difficulty is overcoming the need we seem to have to want to measure things, to predict. We cannot predict higher order abilities such as capability any more than we can predict creativity. We obtain the skills and knowledge to be a painter but a “work of art” is another issue.
The challenge is to implement processes designed to create optimum conditions for making decisions in the face of new and unforeseen problems. This can be described as fitness of purpose rather than fitness for purpose. Documenting the process so we can learn from it might be the best we can hope for (Stewart Hase & Tay, 2004).

Evaluating the work of Dick (1997a; 2000a; 2001), Davis and Hase (1999), Flood (1999), Revans (1980; 1982; 1998), and Tay (2003), action learning and action research are found to be suitable approaches for achieving the competency pursuits in complex environments (Stewart Hase & Tay, 2004).

In a separate study, Denning evaluated the language-action philosophy and established the importance of understanding how language acts in relation to competency and trustworthiness.

We all want to accomplish what we set out to do. Our accomplishments constitute our base of experience and allow us to move to higher stages of competence over time. The more competent we become the bigger the accomplishments we can achieve and can aspire to.

Language-action philosophy uncovers the truth that accomplishment cannot happen without commitments. Commitments are linguistic acts. The more we understand about the language acts in coordination, generation of possibilities, and disclosures, the more we will be able to organize ourselves to accomplish our goals. Most people report that the language-action perspective, by revealing new and effective actions, has enabled them to become more competent and trustworthy. They gain a competitive edge relative to others who lack this interpretation.

The language-action perspective illuminates many other phenomena of interest to professionals: for example, the meaning of innovation and how to produce it; the meaning of research and its connection to innovation; power and its influence on actions; entrepreneurship; design; and (for computing professionals especially) information (P. J. Denning, 2003).

In this regard, the establishment of an action learning session for the IRM staff was an appropriate step forward to instill a process for knowledge sharing and learning. Formalizing the IRM program as a process in the organization, since the beginning of this study, further provided the environment for developing IRM competency.

At the stakeholders’ end in the line-of-business, in most situations, staff members were committed to do a good job to make sure that adequate security controls were
designed, implemented, and/or delivered as part of their work. However, they often lack the competency to do it, and capacity to execute their commitments. Investing in training people and creating an environment conducive to gaining the competency were therefore necessary.

4.3.1.4 Five-level Action Map (FLAM)

Reflecting on the reflections of the two action research sub-cycles in implementing the Model A approach in organization ALPHA, a strategy action map for an information risk management system evolved as an initial outcome of the study.

The “Five-level Action Map” (FLAM), as the name suggests, consists of five levels of possible action strategies. The first three levels form a hierarchical structure, whereas the fourth and fifth levels exist in all the first three levels, and are also inter-related, as shown in Figure 21.

1. Strategic or management level, in which the organizational and reporting structure, roles and responsibilities, policies, risk philosophy, and principles of practice should be designed and developed.

2. Program level, in which a series of programs should be identified and designed to address the current issues, with longer-term objectives of information security risk management.

3. Project level, where each program may comprise of one or more projects, with the assignment of ownership, allocation of resources, determination of schedule, and implementation so that the program will eventually become operational and exist as part of the organizational system.

4. Technical and process/workflow level, whereby the technical infrastructure, components, and related processes and workflow are determined, developed, and implemented as part of the programs, in the form of projects.

5. Event level, whereby both planned and unplanned (for example, emergency incidents) can be dealt with programmatically, or through some form of organizational preparations upon their occurrence, either as part of, or outside the programs. The idea of including an event level in this action map was triggered by the learning from the occurrence of the SNMP and SPAM incidents as discussed in Section 4.2.6 and 4.2.7.
The action strategy in each level requires its own set of plans, personnel competency, timeliness (or timeline and schedule), processes, and technology support to ensure its ability to meet its objectives, and collectively the objectives of the upper level.

Analyzing the application of action map in Figure 21 in the action research cycles further revealed that there should be an inherent relationship, or influence between the technical and process level and the event level, and vice versa. In other words, the technical infrastructure and processes implemented as part of the program would either support or hinder the responses and management of events. In essence, the second research question showed the needs for this requirement (for events) to be addressed as part of the strategy or program, because events are in fact those changes that affect the risk environment.

4.3.1.5 Combining social and technical aspects of information security risk management systems

Another outcome of the social-technical approach was rationalization of the systems of information security risk management practices into an integrated process as shown in Figure 22 (J20060819). The systems combined the approach that was developed, integrating the use of available tools and processes from pre-merger organizations, and the measurement system implemented by the global IRM group.

A key difference between the information risk management systems depicted in Figure 22 and the previous approach (as shown in Figure 11) was the inclusion of the key stakeholders as part of the systems. They were: the information owner, line-of-
business application development teams, IT services, and members of the various management-level councils and committees. The top of the diagram depicts the high-level processes for information risk management. The system starts with an Information Security Risk Assessment (ISRA)\textsuperscript{105} process, followed by risk review, updating of the scorecard, devising and acting on the remediation plans. The cycle repeats with more reviews, and, on a regular basis, revisiting the ISRA process itself to make sure that previous assessment of the individual application remains valid, or otherwise, updating it accordingly.

The rectangular boxes (colored red) in Figure 22 denote activities involving respective stakeholders and IRM. These red boxes are critical junctures that involve both social and technical activities, requiring IRM to use social knowledge, tools, and skills to understand and address stakeholders’ concerns and agendas, and influence their acceptance and support in order to achieve the desired outcome at those stages. Techniques adopted included stakeholder analysis (S), entry and contracting (E), convergent interviewing (C), dialectic data analysis (D), and Flood’s Four Windows systems view (4), which were found to be effective to address the “soft” issues and needs in the information security risk management systems processes. These techniques are labeled as “SECD4” in the red boxes.

Figure 22: Information risk management systems incorporating stakeholders’ participation
The SECD4 social-technical process prior to the presentation of the various scorecards and reports to the IRM Risk Council, Line-of-business (LOB) Technology Control Council (TCC), and Location Operating Committee (LOC) was updated as part of the system to socialize the scorecards and reports with the individual stakeholders in these councils/committees to maximize the acceptance/agreement prior to the actual meeting, and minimize surprises to all stakeholders involved.

In reviewing the literature relating to information security risk management, one of the propositions (in Section 2.8) was that:

The two aspects—social and technical—were co-producers of the intended outcome of information security risk management. The distinctive characteristic of each must be respected or else their contradictions will intrude and their complementarities will remain unrealized.

The outcome of the information security risk management systems as depicted in Figure 22 indicated that a social-technical integrated approach was possible, and necessary, in order to understand and address the stakeholders’ concerns and requirements throughout the life-cycle processes involved. As Peter Drucker asserts in the context of managing the performances of non-profile organizations:

I soon learned that [successful executives] start out by defining the fundamental change that the non-profit institution wants to make in society and in human beings; then they project that goal onto the concerns of each of the institution’s constituencies (Drucker, 1990, p. 111)

IRM’s mission and goals were related to the “fundamental change”. The social-technical integration in IRM systems, which brought forward the needs for stakeholders’ acceptance, commitment, support, and satisfaction were related to the latter, i.e., addressing the “concerns of each of the institution’s constituencies”.

4.3.1.6 Communicating Information Security Risk Status

The learning from this action research sub-cycle (J20060819) and the updated IRM systems shown in Figure 22 highlighted that one of the key elements in the systems was the IRM scorecard\(^\text{106}\), introduced as a tool to determine IRM performance in each LOB and location. The aggregation of the scorecard of each LOB provided a higher-level organizational unit view of the information risk control status, including its state of implementation across the lines-of-business and locations, regionally and globally.
Using the scorecard as a focal point for performance measurement relating to risk control resolution in the Tokyo office in organization ALPHA over a period of three months helped to reduce the number of high risk (“red”) issues from 12 to three. This showed the focus that the stakeholders had given to the issues highlighted in the scorecards and presented in the LOC (J20021012).

The scorecard, however, only captured issues relating to the IT Control Policies implementation and compliance. From a risk perspective, the controls (specified in the IT Control Policies) reflected the risks that were assessed when the policies were being formalized, but not those risks that emerged thereafter. In particular, risks emerged from the changing IT and operations environment, such as increasing use of Internet-enabled applications, IT outsourcing, and business operations offshoring. New security issues, including those that were reported by the CIRT function, with a security advisory issued, could not be captured in the scorecard.

From a management perspective, there is a difference between control and controls. Peter Drucker clarifies this as follows:

> In the dictionary of social institutions the word “controls” is not the plural of the word “control”. Not only do more controls not necessarily give more control, the two words, in the context of social institutions, have different meanings altogether. The synonyms for controls are measurement and information. The synonym for control is direction. Controls pertain to means, control to an end. Controls deal with facts, that is, with events of the past. Control deals with expectations, that is, with the future. Controls are analytical, concerned with what was and is. Control is normative and concerned with what ought to be (Drucker, 1973, p. 494).

This means that the organization’s IT Control Policy was essentially specifying the ultimate state of security that the organization aspired to achieve—a vision of control. However, the policy is static, but the environment involved is constantly changing—dynamic. As such, the vision of control promulgated in the policies, which can only encompass known risks but not issues that are new or unknown at the time of its formulation, was limited to a known risk environment.

Given that the scorecard was capturing the status of implementation and compliance against the IT Control Policy, it was measuring the state of controls that had been achieved (in the case of amber and green items), or not achieved (in the case of red items) against a known risk environment. In other words, the scorecard could not
provide the control as desired from an information risk management perspective, which needed to address both known and not-yet-known issues (including emerging risk issues), even though it was effective in bringing focus on key risk issues.

A security control such as an incident response procedure might have been implemented, and therefore could score a green rating in the scorecard. The line-of-business and IT Services, however, might not be able to respond to an actual security incident when it involved an attack on a vulnerability that was newly discovered, where the security patch was not yet available, or workaround (i.e., tactical security controls) had not been identified. Such issues had arisen in the organization previously (such as the SNMP vulnerabilities and SPAM incidents), but could not be captured in the scorecard. Given that the scorecard measures only against predetermined controls specified in the policy, the scorecard was blind to new issues, and therefore not responsive to change, and not reflective of the actual risk situation faced by the organization.

While the scorecard had helped to make a positive impact in gaining LOB stakeholders’ support for the IRM program, the compliance nature of its contents were raising new issues at the same time. As noted in the annotations and data analysis of this research cycle (J20060819), some stakeholders were more concerned with the colors in comparison with other LOB, in particular, IT Services, than the underlying issues. This caused distraction, and at times influenced the outcome of the scoring, and the efficiency of the process as a whole. When the scoring was affected, the eventual remediation plan and action strategies were also affected. This could result in developing incomplete remediation plans and action strategies, and consequently retaining the underlying issues that were side-stepped as a result of the stakeholders’ personal interventions and IRM staff members’ lack of assertiveness in ensuring an accurate and objective score was made in the scorecard.

If consistent improvements in the scorecard results has been achieved, as was shown in the case of Tokyo’s use of the scorecard in performance management, and IRM members had been active players in making the change in the business to bring about those improvements, then the outcome of the risk status of the business as reflected in the scorecard would be indicative of IRM’s contributions.
An issue emerged when the scorecard showed a decline in performance (having more red and amber issues). Could IRM be one of the stakeholders accountable for the poor performance reflected in such a scorecard result? This perhaps required more evaluation before its relevance could be determined, since there were a number of possibilities for lowering the risk status:

1. If the resolutions recommended by IRM members were ineffective, IRM should indeed be accountable.

2. If the resolutions recommended by IRM members were effective, but the outcome was affected negatively by errors in practice by the end-users in the business, then the end-users should perhaps be responsible. However, if the error was introduced as the result of an incorrect instruction from an IRM member (say during a training session), then again, IRM members might have been accountable.

3. If the lowering performance captured in the scorecard was a result of the changing environment, or the step-up of more risk assessment activities, which the scorecard could not reflect effectively, it would be difficult to assess the factors contributing to the negative outcome.

IRM’s accomplishments were also dependent on others in the lines-of-business and IT Services’ fulfilling their commitments to the remediation plan and actions. Their failure to deliver something important is likely to also prevent IRM staff from delivering something they had committed. To improve the organization’s IRM performance and risk status therefore requires more than establishing the ground rules of practice for the IRM. As noted in the discussion on competence and trust (Section 4.3.1.3), the ability to execute and delivery a commitment is also dependent on the competency of the LOB and IRM staff members involved. Their efficacies therefore cannot be measured simply through a reductionist approach, such as the use of a scorecard.

Even if the above issues relating to negative outcomes could be resolved, the fact that the scorecard could not capture issues relating to changes in the risk environment, in particular externally generated changes and issues, the organization could still suffer from events relating to such changes. In such an instance, the scorecard would be
redundant, but IRM would still be required to respond to the events to help the line-of-business manage the risks.

Consequently, using such a scorecard as a performance management tool for managing IRM members’ efficacy is subjective and therefore limited, even when additional investigation is conducted about individual negative outcomes to determine the actual causes when lowered performance has been reported.

Given these limitations, an alternative method or methods needs to be identified or devised, tested and evaluated in response to the research question about IRM performance measurement.

More importantly, the analysis above also showed that the scorecard system as used in organization ALPHA, would continue to drive a culture of compliance, focusing on control-oriented security, but unable to deal with the security challenges in a constantly evolving and changing business and IT environment. This disconfirmed its suitability as a tool for managing information risk in response to the first research question discussed in Chapter 1.

4.3.1.7 Limitation of the new IRM systems

One of the key features of the new IRM systems introduced through the Model A Approach was the introduction of the “proactive detection of weaknesses” process. The proactive detection process was identified from the causal analysis of the IRM systems against the previous version (as depicted in Figure 11.) Its objective was to provide a filter against complacency, and to ensure that the introduction of any new projects, technologies and business initiatives to the environment would be risk managed before implementation. The aim was also to eliminate the “pre-audit” practice, and to ensure proactive management of information risk.

While the name of the process contained the word “detection”, the actions that can be taken were on two sets of activities—a scheduled set of risk reviews activities, and a comprehensive awareness program. The awareness program were focused on developing and increasing people’s awareness of information risk and commitment to practices that would help to identify and detect security weaknesses in their business systems and practices, rather than relying on IRM or other third parties to detect those weaknesses.
While awareness has been a common suggestion for improving security practices—for example, see Parker (1998), and Hinson (2005)—improvements resulting from awareness have also been found to be subjective, depending to a large extent on the contents presented, and the motivations for learning (Siponen, 2000a). As highlighted in Wilson and Hash, “the purpose of awareness is to focus attention to security.”

Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly (Wilson & Hash, 2003, pp. 8-9).

In many cases, learning through an awareness program cannot be accurately quantified and qualified, except for those that are focused on a specific skill set relating to a well known set of risks or errors. With staff turnover and business environment changes, re-training is also necessary to keep everyone updated. This means that the organizational capability in detecting risks by individuals will be subjective unless it is limited to a specific scope of known risks, and regularly tested against a pre-determined set of criteria. The effectiveness and efficiency of such efforts is therefore limited.

Reviewing the literature available also identified this as a gap in the knowledge domain at this juncture, as the concepts, ideas, and recommendations available on the topic of detection were focused on technical measures such as security monitoring and intrusion detection systems—for example, Graham (1998), Northcutt (1999), Bace and Mell (2001), Grance, Hash et al. (2003), Frahim (2005) and ISO (2006)—but were not based on an information risk management perspective, on how people and/or organizational systems might play a role in achieving such a requirement (except for imparting and improving individuals’ security awareness). Siponen (2000a) also discussed the motivation for security awareness training, which is often aimed at achieving an effective performance level measured against specific security guidelines or standards adopted by the organization to enhance security practices rather than to improve risk detection capability, in particular, in relation to changes in the risk environment.

From a technical perspective, as noted in Ptacek (1998), Bace and Mell (2001), and Frahim (2005), there are also several security limitations in an intrusion detection system (IDS) as well. An IDS system may be rule-based, or network/system behavioral based. In both cases, only known attacks, or patterns of attacks, bad or suspiciously bad traffic will be stopped. New attacks will therefore be missed by such
detection systems, especially those that are targeted at overcoming the intrusion detection system itself. Graham (1998) and Bace and Mell (2001) added that many IDS are also known to suffer from resource issues, problems operating in a switched network, and accuracy and timeliness of their attack pattern databases. Clearly, relying on a technical approach for detection of security issues will also have limitations. It was also deemed inadequate, as the issues that were of concern include human issues, such as complacency, and management-related ones, such as failure to ensure new projects and business systems are adequately risk-managed.

This analysis suggested that from the systemic perspective of information security risk management systems, a balanced system (i.e., risk-managed system) requires more than introducing a continuous security risk review program and a security awareness/education program. Technology-focused solutions were also assessed to have limited effectiveness.

4.3.1.8 Learning about information security risk management through the “Model A Approach”

At the end of the second action research cycle, I conducted another stakeholder analysis of the stakeholders in ALPHA whose actions could have direct or indirect impact on the IRM program. The outcome (depicted in Figure 23) showed progress in having more stakeholders supporting the new IRM Program, demonstrating the positive outcome of the social-technical approach adopted.

![Attitudes towards IRM Function](chart.png)

<table>
<thead>
<tr>
<th>Attitudes towards IRM Function</th>
<th>Number of Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly in favor</td>
<td>7</td>
</tr>
<tr>
<td>Slightly in favor</td>
<td>28</td>
</tr>
<tr>
<td>Indifferent</td>
<td>27</td>
</tr>
<tr>
<td>Slightly opposed</td>
<td>8</td>
</tr>
<tr>
<td>Strongly opposed</td>
<td>2</td>
</tr>
<tr>
<td>AR1</td>
<td></td>
</tr>
<tr>
<td>AR2</td>
<td></td>
</tr>
</tbody>
</table>

Figure 23: Progress in stakeholders' acceptance of IRM Program
While progress was made, the analysis also revealed that business resource constraints were a common theme that slowed the progress of implementation of activities relating to the IRM Program, in the lines-of-business where remedial actions were required. These finding further supported the need for IRM to continue engaging stakeholders in the lines-of-business more proactively, using more social techniques, such as Entry and Contracting (Dick, 2002c) skills to negotiate commitment in addition to roles and responsibilities in each cycle of the IRM review activity.

In the second action research sub-cycle, the model was strengthened with the development and implementation of an evolved approach for identifying key risks, and for addressing them in a programmatic manner. The approach encompassed the methods required to address the social aspects of risk management, deriving a social-technical system as shown in Figure 22. The system incorporated a control scorecard system introduced by the global IRM group as a performance measure for tracking the status of control implementation in the organization. The scorecard used in the model was, however, disconfirmed to be a sufficient tool for managing the performance and efficacy of the IRM program and related sub-systems, given its limitation to only predetermined controls specified in the IT Control Policies, and blindness to new and emerging risk issues in the changing business environment.

The outcome of this research cycle was further influenced by more changes in the organizational environment. This included outsourcing and offshoring initiatives, which both required the IRM program and model to be more flexible and responsive. Change was again identified as a key attribute that would influence the efficacy of the IRM Program.

Through the research cycle, the following shortcomings were identified. These shortcomings constrained the applicability of the model to situations where the risks were known and documented:

1. Although this model incorporated a component to address unplanned events (from the learning about related incidents during the sub-cycle), at this stage, a method for realizing this could not be found or developed. This was partially due to the organization’s focus on the remediation of known risk issues, and addressing audit compliance issues. At the same time, no suitable methods could be found in the literature or from other practitioners to address this need;
Chapter 4 – Data Analysis, Interpretations, and Findings

2. In terms of detecting emerging risk issues, the Model A Approach relied only on peoples’ awareness as the main mechanism to identify and report observed unusual events in their areas of work.

4.3.2 Model B Approach

Several key stakeholders attributed the inadequacies of the Model A Approach as an organizational discrepancy, in terms of the reporting structure. A revised model, known as Model B was therefore proposed and implemented. The revision focused on the organization structure, decentralizing the IRM function to become part of individual LOB, with the regional and corporate (global) IRM function becoming respective coordination points to ensure consistency of practice and assist in resolving cross-LOB risk issues.108

4.3.2.1 IRM organization model

Analyzing the changes of the IRM organization model against the Balanced Scorecard (Kaplan & Norton, 1996, p. 62) strategy developed in the previous cycle (J20020826), the primary outcome of the change was the cost model for supporting the IRM function. On the surface, the risk management model was not impacted. The various functions and initiatives that supported the strategy remained the same, although the line of responsibility and accountability were transferred to the line-of-business (LOB).

From a global organizational perspective, the organizational model, while decentralized, had two models in one. At the global level, the model exhibited a form of “federated organization”, as described in Charles Handy (2002), which has a small core (corporate IRM), and multiple subsidiaries (which were the respective LOB IRMs). For a federated organization to work, Handy highlights two principles that must be understood and practiced:

The first is subsidiarity: the principle that the larger and higher body should not exercise functions which can be carried out efficiently by smaller or lesser bodies.

The Corporate IRM function was similar to the higher body.

The second principle refers to those in the subsidiaries: they must want to increase the range of activities in their roles.
The LOBs were receptive to the idea of taking over the IRM function as part of their business. The Global LOB IRMs were willing to increase their range of activities involved as part of the scope of work.

As such, the new IRM organization model satisfied these two principles at the global level. As noted by Pugh & Hickson, for the federated model to work:

A considerable amount of trust and confidence is required. The centre cannot be sure if the subsidiary organization can carry out the function efficiently before it has actually done so. But, in a catch-22 situation, if it uses this lack of experience as an argument against allowing them to try, then subsidiarity will never occur (Pugh & Hickson, 1996, pp. 41-42).

The second principle further implies that a model provides “more discretionary opportunities in the job, which no one has specified, but, if carried out effectively, will be regarded as showing appropriate initiative” (Pugh & Hickson, 1996, pp. 41-42). There were therefore clear benefits to IRMs in the LOB if the model was well executed.

At the regional level, although IRM would have liked to believe that the group had similar autonomy for each LOB IRM sub-group in the region, the reality was that the LOB IRM members in the region were members of the larger LOB IRM group at the global level. As such, they did not have the prerogative to make decisions and set directions of their own locally, but had to follow the strategy and plans of the global Head of LOB-IRM within the LOB. This, essentially, was a de-centralized, hierarchical structure, within each LOB IRM organization. The regional IRM group that was “loosely” formed through the matrix reporting lines established was an organization that had three reporting lines for each IRM. The three reporting lines were: (1) global Head of LOB IRM; (2) Regional Information Risk Officer (RIRO); and (3) regional LOB CTO or Head of IT. RIRO, as the main coordinator for IRM plans and activities within the region had to synchronize them with seven global Heads of LOB IRM, and at the same time to ensure that the seven regional LOB CTOs were agreeable to those initiatives. This created substantial complication for the IRM organization itself.

Using the dialectical analysis approach on the data collected, as in the previous research cycles, a number of shortcomings were identified, as compared with the
organizational structure in the “Model A Approach”. The following summarizes the shortcomings recorded in my research journal J20020422 (edited).

1. While cost management was one of the motivating factors for the change, the implementation had, however, resulted in additional cost (directly incurred by the businesses) in the number of headcounts. There were seven global Heads of LOB IRM at this stage, re-leveled to positions of Senior Vice President, instead of Vice President, and the LOB could no longer work on a partial headcount basis by sharing IRM resources with another LOB. The minimum IRM headcount an LOB had to have is one staff. Before the re-organization, several LOBs were only funding half or less headcount resources for the regional IRM group;

2. Even though the total number of IRM members in the Asia region, as a result of the re-organization, had increased (from 14 to 17), the group could not be scaled to cross support different LOBs. Some IRM (for the less critical LOB) had fewer activities due to the lower number of business applications involved, and also the more static nature of those applications (like accounting and human resource systems). Others, however, continued to be challenged by more changes in business applications and regulatory compliance. There was also no motivation for IRM staff members from one LOB to provide support to another LOB, as they could be held accountable for negative outcomes, but not recognized for positive results. The resource-sharing issue was played out when one LOB was required to conduct a security review for an outsource service provider (OSP) that was located in Singapore, but he was based in Hong Kong. A number of other OSPs used by the Investment Bank LOB were also located in Singapore. In the “Model A Approach”, an IRM member in Singapore could simply be assigned to review all the Singapore-based OSPs without the need to be concerned with the cost issues relating to a specific LOB. In this case, the IRM in Hong Kong had to justify a single trip to Singapore just for the review, and the Singapore-based IRM (who were non-CBS IRM staff) could not extend their assistance to perform the review. From a risk management perspective, the partitioning by LOB further reduced or limited the view that IRM could gather about the risks relating to OSP. These
views had to be aggregated separately through the global IRM scorecard process instead;

3. In terms of IRM practices, maintaining consistency across different LOBs now emerged as another issue. In the “Model A Approach”, every LOB IRM was already planning a specific approach for managing risk, mitigating gaps and issues, and using different reporting and assessment tools. Much time and resources were invested to bring about more consistency. With the change, the LOB IRM would be more focused on fulfilling the demands of the regional CTO and the global Head of LOB IRM, instead of ensuring consistency of practice across IRM as a group. Although a global IRM Technology Risk Council (TRC) was established to promote consistent practices, the recommendations from the Council were not enforceable, both from accountability and resource perspectives. The Council could only influence the principles of practice in general, but not how the practice was going to be executed on the ground;

4. The inconsistency of practices had the potential of causing confusion to businesses and the auditors. It could also lead to different interpretations of policies;

5. As the number of IRM staff in each LOB was limited, each LOB IRM would have a broader scope of responsibility and coverage. This gave little room for specialization. IRM staff members would therefore become more generalist risk managers, and more external assistance would be needed on newer issues. This would impact on IRM career development, as well as increase the cost of risk management;

6. The global LOB-alignment also meant that every risk decision in the region (within the LOB) would need to have the global Head of LOB IRM consulted. The turnaround response time for IRM would therefore be longer. When priorities on the global side started to shift, the region’s attention would also be affected. Essentially, if LOB IRM could not tap into other local or regional IRM resources, the LOB risk exposure might be higher;

7. As a direct cost to the LOB and reporting directly to the CTO in the LOB, IRM members would have to be more business-result focused. While this
might provide a better understanding of the business that they were serving, it also meant that IRM would avoid contentious issues that could be seen as not being business-result oriented. This was also related to the issue of habituation, which is analyzed in the sub-section below.

Analyzing using Flood’s (1999) Four-windows perspective, the issues and dilemmas had the potential of affecting all four areas unfavorably.

1. The issues and dilemmas of consistency of practices, increasing cost and reducing scalability of IRM resources, increased complexity and bureaucracy in reporting and issues and decision escalation would affect the structure of the systems, and hence the effectiveness of the IRM group;

2. The issues of cost versus scalability, and increased bureaucracy further affected the systems of processes, and hence the efficiency and reliability of the group;

3. The difficulty in cross-LOB support would reduce the interactions between IRMs and also the opportunity for new learning from other LOBs IRM and related issues. In addition, from the systems of meaning perspective, the limitation on IRM development and the generalization of IRM expertise further diminished the meaningfulness of IRM work and practices;

4. Finally, from the systems of knowledge-power view, the question of fairness of the new organization to the LOB with the increased cost of managing information security risk had to be considered. Furthermore, one had to also question whether it was fair for LOB IRM at the local level to undertake a much greater range of responsibilities when she was not supported with adequate resources to execute those responsibilities. The fairness of LOB IRM recommendations to the organization for resolving risk issues identified at the LOB also had to be questioned, given the bias of LOB IRM reporting and the reward system in the new organization.

As such, from the Four Windows systems perspectives, the change did not add significant value to the IRM systems. The “Model B Approach” introduced several new issues and dilemmas without substantial benefits compared to the “Model A Approach”.

186
4.3.2.2 Learning about information security risk management through the “Model B Approach”

The implementation and execution of the “Model B Approach” raised a number of issues and dilemmas as highlighted in the discussion on the “IRM organization model” above, these showed that the approach was ineffective in improving the risk status of the organization and the systems for managing information security risk.

More critically, the analysis of the changes, whereby IRM become an insider in the LOB, like the CSA process, had the potential of introducing the risk of habituation, which was an issue identified earlier in Section 4.2.4. When such an organizational model is in use, additional measures need to be taken to counter the habituation challenges.

The learning and analysis from negative cases evidenced in the research cycle disconfirmed the value and usefulness of the “Model B Approach” from an information risk management perspective, as well as from a cost and resource management perspective. The “Model A Approach”, which had many component parts developed and evolved over the period of the study, provided a valid social-technical framework to address the information risk issues and dilemmas in the organizations.

4.3.3 Learning from the SQL Slammer, Blaster Worm, and SAR incidents

The real test of any approach or model of information risk management occurred when the organization encountered a significant security and non-security related event that have an effect on the organization risk status. During the action research cycles in which the two social-technical models were implemented and tested, the organizations were faced with the (1) SQL Slammer network worm; (2) Blaster network worm; and (3) Severe Acute Respiratory Syndrome (SARS) epidemic incidents.

While the social-technical approach (Model A Approach) was able to help address the “soft” issues in the organization, the techniques were concerned about understanding stakeholders’ perspectives and gaining their commitments to actions, but not in preparedness or readiness for the change events and related incidents. Therefore,
when these incidents occurred, the responses were again reactive, focusing on recovering rather than limiting the damage as the events unfolded. Besides a poor state of preparedness, these incidents showed a lack of capability and capacity to respond.

As noted in the research logs (J20030422-3, J20030818), following the SQL Slammer incident, the global IRM group proposed an update of the IT Control policies requiring third parties’ access to the corporate network to be from a “certified” computer system only. However, at that point, there was no technology available to detect an authorized computer system connecting to the network. The only possibility was to use a fixed network address, and/or a fixed hardware identifier for the network access card on the system. This was assessed to be impractical from an administrative standpoint, due to the large number of computer systems on the network (with more than 100,000 staff worldwide). Without the capability to detect a violation, the policy could not be enforced, even though a process for certifying third parties’ computer systems could be implemented. Nevertheless, the certification process was still under discussion when the Blaster incident occurred (which was more than seven months after the SQL Slammer incident).

For convenience and expediency of services, contractors, consultants, and even staff members, continued to connect to the corporate network any machine that they needed to help them deliver the services that the organization required. They would get a monetary penalty for not delivering the services, but the chance of a virus or worm attack being traced back to them was low. They would also claim ignorance of the policies and certification process when they were found to be using uncertified systems on the network. Finally, when a certification body exists to perform the validation work, the certification body needs to provide evidence of proper validation being conducted, and the state of the machine configuration upon completion. The certification process could not ensure that the user of the machine will not add or remove other software and devices to the system after the certification was completed.

Another concern about the policy was the definition and implementation of a “secure build” that was required to ensure that the third parties’ computer system connecting to the network was not infected, malicious, or vulnerable by itself so that it could spread them to other systems in the corporate network. Ideally, the secure build should be able to detect both new and previously known risks on the system that was
going to connect to the network. However, the technical measures, including software and configuration that can be implemented at the time of this research cycle (in 2003), were limited to those for preventing known risks of attacks. Anti-virus software, which was the main security technology relied upon to secure the machine, can only detect previously known viruses and worms, not new strains that have just been released in the wild. When a heuristic, non-signature based, virus protection capability was used, it tended to take a more precautionary approach, often result in false alarms. As such, their sensitivity to the differences was reduced in order to gain users’ acceptance—another form of habituation (Section 4.2.4) imposed.

As such, the new policy, even with the certification process in place and secure build made available, was not sufficient to provide the controls needed to respond to such unplanned events.

On the technical issues underlying the SQL Slammer and Blaster incidents, both worms exploited vulnerabilities that require access to network services (NetBIOS, and SQL) that should not be opened to the public on the Internet. A security solution for providing those services in a secure manner (via application proxy), which was available commercially to prevent external exploitations, was, however, not deployed. This showed a lack of security consideration during the design of those applications that require those network services to be open publicly. In both cases, security patches were already available many weeks before the worms were released, but they were not applied. This showed the ineffectiveness of the patch management systems that had been deployed in IT Services, which was confirmed in the post-incident review.

As also noted in the post-incident review after the Blaster incident, ineffective communications and inaccurate inventories of IT assets and policy implementations were the major obstacles to effective response and also managing the recovery. These findings should have surfaced in the SQL Slammer incident, but no post-incident review was conducted by IT Services then, again indicating possible “learning disability” (Argyris & Schon, 1991b; Senge, 1990, pp. 17-26) in the organization, as also discussed in Sections 4.2.6 and 4.3.1.2.

When a perpetrator has developed an exploit code and launched a virus or worm program to attack vulnerable systems on the Internet, either behind or outside the corporate firewall networks, the attack pattern will be copied by other perpetrators.
From an information risk perspective, we should therefore expect similar or evolved types of attacks to recur. These are expected events that organizations must at the minimum prepare against. The recurrences of similar events are not coincidences. As Edward B. Burger and Michael Starbird highlighted, they are “expected coincidences”, since there are huge data about such attacks once they have occurred, and results and impact have been demonstrated.

Coincidences do happen, and when they do, we take note. Any particular coincidence is indeed an extremely rare event; however… what is rarer yet is for us to experience no coincidences at all. Basically, the moral is to expect the unexpected (Burger & Starbird, 2005, p. 4).

Besides catering to the expected coincidences, we need to also expect the unexpected (like the occurrence of the SARS epidemic, which lasted several months, affecting also the infrastructure systems in ways that we did not anticipate).

On hindsight, the SARS incident should also have been considered an expected coincidence since the Avian Influenza (“Bird Flu”) incident had occurred in Hong Kong in 2002, causing the culling of more than 170,000 chickens to eliminate any possible strain of the virus from evolving into an epidemic (CNN, 2002). The BCM function did not envisage after the Bird Flu incident that an epidemic could result and impact business organizations directly. The SARS epidemic thus became an unexpected event that no organization was ready to respond to, including healthcare providers and medical professionals.

In a Global Information Security Survey involving more than 1,300 respondents in 2005, Ernst & Young LLP (2005) reported that organizations, on the average, allocate only 15% of their time and budget for incident response-related activities when attacked, but 38-41% for daily routines, and 18% for compliance, 6-7% for others, and 18-22% for strategy.

In the same survey, Ernst & Young LLP established that 60% of the respondents named “compliance with regulations”, 31% named “worms and viruses”, and 55% named “meeting business objectives” as the main driver that most significantly impacted or would significantly impact organizations’ information security practices.

The lack of focus on incident preparedness or readiness was therefore a common problem in the industry, not peculiar to just organization ALPHA. From an
information risk management perspective, these incidents substantiated the need and importance of an event level action strategy in the information risk management model developed in the earlier research cycles.

### 4.3.4 Reconsidering information risk management with business continuity and disaster recovery planning

While the SQL Slammer and Blaster incidents revealed the organization’s inadequacies in responding to information security risk issues, reflecting the SARS incident provided new insight into the workings of BCM, including the organization’s business continuity plan (BCP), and disaster contingency and recovery plan (DCRP).

As shown in Figure 24, and reviewed in Section 2.4, the traditional approach in information security planning was often based on a strategy of protect, detect, and respond or react. Most organizations such as ALPHA, however, placed significant focus and emphasis on the protective element, in view of the regulatory and auditors’ push for compliance. While incident detection, respond, and management were part of the IT control policies, the systems for detection focused mainly on known events, and the systems for response management were focused on recovery.

In most cases, as in organization ALPHA, recovery of IT infrastructure and application systems was regarded as part of IT management, and therefore undertaken as a sub-function of the IT Services division focusing on DCRP.

![Figure 24: Lack of synergy between IRM, BCP, and DRP systems and processes](image)

As for recovery of business-related services, they were to be undertaken by the Business Continuity Management (BCM) function, as part of the BCP process.
As shown in Figure 24, IRM can be implementing many security measures to prevent an incident from happening, but when an incident does occur, it often cannot react on its own. If it is a security event that affects the IT infrastructure or systems, IRM has to call upon the disaster contingency (severity management) process, with actions determined by the DCRP management. In the case of a business operation or service issue, the IRM’s React/Respond element will route it to BCM to determine what business continuity steps are to be taken. The role of IRM takes back seat, providing on-demand advisory, mainly with regards to whether the IT control policies can be relaxed to meet the needs of the incident situations. IRM plans and actions prior to any incident do not provide guidance or training, or implement any systems or processes that can facilitate swifter response or faster recovery. These were in fact the outcome experienced in the series of incidents that occurred at this stage of the research study. Clearly, there were gaps, or a significant lack of synergy among the three roles that were all concerned with unplanned events affecting the organization.

4.3.5 Summary of issues and dilemmas and research outcome

Table 2 summarizes the key issues and dilemmas analyzed and interpreted in this research cycle involving the development and implementation of Model A and Model B approaches, using Flood’s (1999) Four-windows systems view.

<table>
<thead>
<tr>
<th>Systems of Process (Efficiency &amp; Reliability)</th>
<th>Systems of Structure (Effectiveness)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The de-centralized organization model (“Model B”) increased overhead in resources and with decision authorities concentrated in global groups could impact on efficiency and reliability of IRM in the region in each LOB.</td>
<td>“Model B Approach” lagged in flexibility, requiring all decisions to be made at the top of the organization hierarchy, in the global groups, and added new layers of coordination and communications requirements in the region and globally.</td>
</tr>
<tr>
<td>Existing systems of processes unable to detect emerging risk issue. Incidents showed the systems of processes were not ready to respond efficiently and reliably to critical security events.</td>
<td>Multiple incidents showed that existing system focus on protection and prevention with little to no attention to responsiveness, resulting in significant losses in productivity and a long period until recovery.</td>
</tr>
<tr>
<td>Gaps in process integration and synergy among IRM, BCP, and DCRP with regard to incident response and management.</td>
<td>Changes in the organization structure did not cater to the need for increased local planning and action strategies, affecting the effectiveness of IRM and</td>
</tr>
</tbody>
</table>
Table 2: Four-windows (Flood, 1999) systemic view of the information risk management situation in organization ALPHA in action research sub-cycle 3

The outcome of the study conducted through the development and implementation of the Social-Technical Approach were:

1. Incorporation of social-science and systems thinking techniques into the IRM system was possible, and from the subsequent stakeholder analysis conducted, had resulted in positive outcome in the acceptance of IRM Program, and also commitments of stakeholders in implementation. Causal analysis of the new IRM system also showed that they were capable of addressing the theory of actions issues among the stakeholders.

2. The FLAM framework and SECD4 process evolved from the learning of the social-technical approach had provided a set of tools suitable for learning and understanding existing IRM systems, as well as devising action strategies for improving organization IRM systems.

3. Care should be taken in the organization structure, as learned from the implementation of the Model B approach, that a fully decentralized model, with full LOB ownership of the IRM function, may not necessarily be efficient,
effective, meaningful, and fair, when evaluated from the Four-windows systemic perspective.

4. The series of security incidents showed that focus on the “soft” aspects of the IRM system is important, but not sufficient, as it does not address the changing nature of the information risk environment, in view of the discrepancies analyzed in the current risk assessment methods, and limitation of a compliance-oriented approach. The incidents also highlighted discrepancies between IRM, BCM, and DRCP functions, whereby the requirements and focus intersected at the response element.

These outcomes suggested the need to further improve the model and approach to address the need to address both planned and unplanned changing events in the information risk environment.

4.4 A Responsive Approach

The initial research cycles established that responding to change was an important issue in the IRM system, and the existing program in organization ALPHA was inadequate to address this need. The need for IRM strategy to focus on preparedness and hence, readiness, to respond did not become obvious until the occurrence of the SNMP vulnerability incident, which was subsequently reinforced when the SPAM, SQL Slammer, and Blaster worm incidents followed. However, as the study then was implementing and testing the social-technical approaches to address the “soft” issues involved in IRM system and program, developing a response-focused approach was deferred.

In realizing the limitation of current approach for BCP and DRP in Section 4.3.4, it was further observed that the common interest or the work intersection between IRM, BCP, and DRP, as shown in Figure 24, is the response element, which exists in all three areas. To close the gap among the three areas, IRM therefore should do something about the response process.

Nevertheless, the notion of “responsiveness” was studied in parallel, and also reflexively debated with fellow action researchers and information security practitioners in the Learning Sets and other discussion forums.
An early discussion on the need to be responsive brought out the concept of piezoelectric when a fellow action researcher related the existence of such a material, known as piezoelectric sensor, and how its internal electrical charges behave in a changing situation detected at its surface (J20020909-2, J20060826). Further investigation of the piezoelectric phenomenon led to the formalization of the piezoelectric metaphor, using it for analyzing the organization, groups, and individuals’ behaviors in various security incidents and disastrous situations, leading to the development of a substantive theory, known here as the piezoelectric theory of information risk management. The piezoelectric theory suggests the development and implementation of a responsive approach, which was supported by case study analysis in organization BETA and the outcome of two additional incidents, and validated through an implementation in organization CHARLIE (J20050711, J20050712, and J20061126).

4.4.1 Piezoelectric metaphor

Piezoelectric sensors offer unique capabilities which are typically not found in other sensing technologies. “Piezo” is a Greek term that means “to squeeze”. When the piezoelectric elements are strained by an external force, say a squeeze or push, displaced electrical charge accumulates on opposing surfaces (PCB Piezotronics Inc, 2002), as shown in Figure 25. This provides the elements with many practical uses, such as pressure sensors, force sensors, and accelerometers that are widely deployed in industrial applications.

The phenomenal behavior of the piezoelectric sensor is interesting in that the charges are displaced uniformly, with all positive charges on one surface, and all negative charges on the other, in response to the force exerted on them. The sensitivity of the material to the external pressure triggers the change (in terms of accumulation of charges at opposing surfaces) in the internal state of the material. The change of states involved in this phenomenal behavior can be summarized into three distinct states: (1) squeeze; (2) trigger; and (3) alignment. When the pressure is released, we get: (1) relax; (2) trigger; and (3) de-alignment.
Contrasting this with human organizations, in the normal state individuals focus on their respective tasks, this is like those charges during a “relaxed” state. When an incident occurs, like the exertion of external pressure on the working environment, individuals who are near to the event will often be those who responded. Unlike piezoelectric material, human responses, however, will be subjective and personal, although they may be influenced by their neighbors, and other personal factors prior to and at the point of the event. The collective responses of all the people involved in the event may range from chaotic to uniformly coordinated, like the piezoelectric sensor.

Chaotic response occurs when the incident has not happened before, or has little resemblance to the prior experience of the people in the situation, and each has decided to take her own action to respond without consultation and co-ordination with the rest. However, if the incident is a repetition of a prior incident, and all the people involved are aware or were previously trained to respond to the type of incident that has just happened, we will likely see similar or near behavior of the organization to the piezoelectric material. This may still vary depending on the willingness and capability of the people involved to respond consistently. Nevertheless, every incident tends to be different, at least partially. The probability of uncoordinated responses increases with the extent of dissimilarity to prior incidents that have been experienced by the people. A small change in an event or a series of events has the potential to result in a different incident altogether. The relationship is non-linear feedback (Stacey, 1992).

To simplify the discussion and analysis, omitting the feedback loop of such a system, we can envisage the state changes from normal to fumble (or confusion) to chaotic resulting from the escalation of the incident variables (both external and internal), from non-incident to critical to catastrophic. The amount of effort (or level of
difficulty) in responding to the incident will increase with the increasing number of variables involved in the incident. The effort required will likely reach a plateau when the outcome is already chaotic. It may even fall drastically at the chaotic stage since there could be nothing that anyone can do at that point. Further changes in the forms and variables of the incident beyond this point are highly unpredictable, so as the potential impact on the responses. As Ralph D. Stacey noted,

> When a system operates in chaos, it is highly sensitive to small changes. It amplifies tiny fluctuations or disturbances throughout the system, but in a complex way that leads to completely different, inherently unpredictable forms of behavior. Because tiny changes, so tiny that we could never hope to notice or measure them all, can so completely alter the behavior of the system, its long-term development depends in effect upon chance (Stacey, 1992, p. 63).

At this point, people tend to work on personal priorities or respond only to their psychological state of mind, immediate in their vicinity, whether to help someone else out of the situation, to work themselves out of it, or simply do nothing. Nevertheless, at this stage, Stacey added, “The behavior of an individual component of a system can have a profound effect on the future of the whole system.”

If individuals in organizations can respond consistently, with close alignment and coordination of each other’s responses, a behavioral equivalent (or near equivalent) of the piezoelectric material may be possible. This requires preparation. Preparedness or readiness of the individuals will also contribute to the ease to respond. The more prepared an organization is to different incident scenarios, the less difficulty it will experience in responding to an incident.

The above analysis inferred that focusing on how to respond, and preparing to respond could potentially be more effective than the existing approach of focusing on implementing controls to protect the organization against undesirable events or incidents. In other words, an organization’s responsiveness (to have its resources aligned) to the anticipated and unexpected behavior (i.e., the triggers) of adversaries, or the occurrence of information risk events therefore relates inversely to the outcome of those actions of adversaries or events on the organization. If this is true, then an organization that is not responsive to the adversaries’ behavior and actions, and related information risk events will more likely experiences a more severe impact than one that is more responsive. While this may appear to be logical,
we cannot be sure that the impact is actually less severe since the nature of the incident is unpredictable in the first place. The study therefore needs to determine whether we are better off being responsive than otherwise.

In essence, response is an action (or a set of actions) to align organization resources to handle a change event. Efficacy of response depends highly on (1) awareness of change occurring or emerging; and (2) awareness of what to do, and be prepared on how to respond to the change detected. As noted in McGee (2004), the choices of actions available to an organization to respond to a change event diminish with time. As the event(s) unfold into an incident, what we can do to respond will become more limited. An early awareness of the change event, and the preparedness, or readiness to act against those changes, enabling the organization to get aligned to the new situation as a result of the change, will make a difference in the outcome of the event(s).

As such, in the organizational environment, there are three attributes in a changing situation, similar to what a piezoelectric material can detect and respond. That is, (1) change events; (2) situation awareness; and (3) critical alignment, as shown in Figure 26.

![Figure 26: Mapping Piezoelectric Behavior to Responsive Approach](image)

These three attributes are key elements of a responsive approach. In other words, to be responsive, an organization needs to have capability to (1) detect and identify the triggers, to discover the change events; (2) prepare the systems (including people, processes, and technology) to respond effectively and efficiently to each different type of triggers—to increase situation awareness; and (3) to coordinate the activities and communicate status of the evolving situation—to align people, process, and technology in the organization system to respond, and manage the incident to provide business continuity, focusing on the critical systems and components involved.

Analyzing this against the past security incidents whereby IRM and the various stakeholders were not able to respond effectively, and the business and IT
infrastructure changes that were initiated by the outsourcing and offshoring plans, it was clear that the changes should include both external and internal events, not just focusing on potentially impactful internal security events.

The organization as a system is complex. While internal changes are being implemented, events that could result in severe security incidents could arise from external events affecting the information systems (and network), or the people in the organization. The span of coverage is broad, across the organization’s infrastructure and application systems. A balance of focus from business can only be achieved if and only if information risk management is focused on criticality of the information risk to the business, and the mechanisms for managing risk have the ability to adapt to the criticality status of the systems and environmental, which varies with time and events in and around the systems. To bring focus, an understanding of what is critical to the business and the supportive services is needed. The potential estimated impact of an event or incident affecting the security or reliability of the systems should contribute to the criticality assessment.

While this approach appears logical, as gathered from further dialogues with external practitioners, questions about its applicability in an actual organizational environment were raised:

1. How to detect and identify triggers that will lead to significant events?
2. If the events are unknown, how can we plan and prepare the systems to be ready to respond?
3. How can we measure the performance of this strategy to know that the organization is ready, since it will be too late to learn about the performance after an incident?

To answer these questions required more understanding of the characteristics of security incidents, and examination of the various forms of incident response that have been practiced. These questions were considered as part of the plan and action strategy in the follow-on action research sub-cycles.
4.4.2 Case Study A: Organization BETA’s approach to emerging risks and attacks

The swiftness in which organization BETA was able to respond to the Sasser worm (Microsoft Corporation, 2004; Symantec, 2004b) incident was unlike the situations in organization ALPHA when dealing with previous worms attacks (i.e., the SQL Slammer (Microsoft Corporation, 2002) and Blaster (CERT/CC, 2003b) worms, analyzed in Section 4.3.3.) Within a few hours of detection, each regional center and subsidiary business location around the world had assembled a local response team to disseminate the security alert to all staff and provide instructions on how to inform customers of the security situation, receive and handle feedback, and escalate infections reported by customers for prompt resolution. The local response center communicates with the global response center via a conference call system, and also electronic mails (emails.) Globally, a security alert mailing system had begun generating alert messages to millions of security contacts in the customer organizations to ensure that they receive the security alert promptly to begin taking appropriate actions. The efficacy of the response resulted in similar swift responses from a majority of the customers contacted, which effectively blocked the worm program from propagating in many organizations. In less than two days, the worm attack diminished to a limited numbers of local incidents.

Internally, within organization BETA, the patch for the vulnerability involved (which the worm exploited) was already installed by all users through the mandatory updating process prior to the worm propagation. As such, the internal network was safe from the attack. The network team however stepped up monitoring of the network to ensure that there were no signs of other attacks emerging during the period when everyone else was focusing on helping customers to respond to the attack.

Three individuals in the corporate group of the company, and two in the regional locations were interviewed and provided input about the processes that had been established, and also how the organization responded in the previous worm attacks, in particular, relating to SQL Slammer and Blaster, in which customers were not as effectively alerted to take actions promptly (J20040510, J20061126). The interviews and documents reviews established that:
1. There were no formal security response processes prior to the NIMDA worm incident in 2001. Subsequently, a much simpler process was established, involving only the security engineering groups, and related product groups in the corporate headquarter.

2. When the SQL Slammer attack emerged, the response team then found difficulties in reaching out to the subsidiary and regional business locations. The security engineering group then began to improve the response process to include dissemination of information to regional and subsidiary business contacts.

3. During the Blaster worm incident, given the scale of the attack, the security engineering response group found it necessary to send the security alerts to all customers organizations directly. It was then discovered that the mailing program was not fast enough in its response (the last customer contact was sent out more than 48 hours after the first alert message.)

4. In addition, not all customer contact information was fully updated, and there was no indication of whether which is a security contact. Most alerts went to the procurement and business executives who were not aware of the security situation and criticality of the alert. Sales and marketing staff in the subsidiary businesses were not aligned to the security situation promptly to alert and help customers on the issues resulting from the attack.

5. The scale and speed of the Blaster worm attack showed that a much more responsive process than the existing security engineering response process needs to be established.

6. After the Blaster incident, the response process and supporting tools were therefore revamped. In each regional and subsidiary business location, a “Security Lead” was appointed. Depending on the size of the business, some of the Security Leads were appointed as a full-time position, whereas others were appointed as a secondary role. The main responsibility of the Security Lead was to ensure security readiness of the region or location.

7. The objective of security readiness was to ensure that the subsidiary and region offices were all ready to respond when the next security related incident strikes and affect the organization and/or its customers. It included activities
such as identifying security contacts in each customer organization; establishment of a virtual security team and a security response team to handle non-incident related security issues locally, and incident related security responses; ensuring all staff undergo security awareness training and understand their roles and responsibilities during a security incident; disseminate monthly security updates to all staff (via the virtual security team); and conduct regular drills of the security incident response process to ensure its readiness. During a security incident, the security incident response team will gather and establish close communications both locally with the local staff, and globally with the security engineering response team. The local staff would ensure all customers under their care has received the security alerts and take appropriate actions. Any issues at the local level were then escalated to the local Security Lead and the global Security Response Lead.

8. In addition to the security readiness program that was implemented worldwide, response tools were also revised with the implementation of a new mailing system and database system that can support simultaneous sending out of millions of emails alerts to customers promptly.

9. In each product group, the engineering and development processes were revised to include a mandatory response process to get the developers and program managers ready to respond to security vulnerabilities and exploits discovered on the products they were responsible for.

The efficacy of the changes made after the Blaster worm incident was demonstrated during the Sasser worm incident. According to the interviewees, the highlight of the changes was the improvement achieved in the communications and message dissemination during the incident response process. In addition, the change was deemed necessary to improve the perception of the organization in terms of its security. Without appointing individuals to focus on security readiness, communications of security alerts and other security messages would be difficult, both internally within the local subsidiary, and externally to the customers (J20061126).

The alignment and preparation of all staff to be ready to respond to any new and emerging security incidents assimilate the realization of the piezoelectric behavior.
During the non-incident stage, internal information security risk management activities were geared towards two major categories of activities:

1. Addressing compliance requirements with regards to the organization’s corporate IT security policy. This included implementation of security technology designed to improve the status of compliance and enable better use of IT systems in the businesses.

2. Preparing individuals and groups in each location and region across the world to be aware of the ongoing security issues, understand the structure, format, and contents of security notification messages (with different level of criticality), and practice the actions desired in accordance to the level of criticality of the security alerts. The latter was performed as part of the incident response drills that were conducted at least every half yearly.

These actions were performed alongside individuals and groups’ day-to-day activities. This stage is similar to the normal, “un-squeezed” (“relax”) state of the piezoelectric sensor.

When a security incident emerged, alert messages were first sent to the security response leads in each location and region to step up their awareness of the situation—improving *situation awareness* as such. Once an incident was confirmed, the communications mechanisms that were established were activated. Security alert messages ready for distribution to all staff and customers were promptly prepared and send to individuals and groups for dissemination. The global security response team was on 24 hours standby to receive calls and emails and ready to take any feedback and accept escalation of issues reported from the customers and individuals across the world. In parallel with all this, the product engineering team worked on the security workaround and updates. Suitable solutions to the incident were incorporated in the security notification messages, and updated as and when new findings and updates emerged.

This stage is similar to the “squeezed” state of the piezoelectric sensor, in which individuals and groups activities were immediately changed to *align* with the needs and actions required for responding to the emerging security incident. As the state of security incident develops, it assimilates the pressure asserted in the “squeeze” of the piezoelectric sensor.
When the security incident was technically resolved with the implementation of the workarounds and/or updates, with a reducing rate of support calls and issues escalation, individuals and groups began to stand down as necessary. The global security response team continued to work with the local security leads to consolidate all reports and lessons learnt from the incident to evaluate the effectiveness and efficiency of the entire system for improvement. Eventually, everyone reverted back to their day-to-day activities as the incident dissolved.

This stage assimilates the gradual release of pressure exerted on the piezoelectric sensor, eventually returning to the normal “un-squeezed” state.

While organization BETA did not devise their action strategies based on the piezoelectric theory, the motivation and learning that led to the development and implementation of a global system of readiness and response was similar to learning and understanding that I had gained while in organization ALPHA. This learning and understanding from organization ALPHA resulted in the formulation of the piezoelectric theory of information security risk management. The piezoelectric theory established that when managing information security risk, the action strategies need to encompass a system of readiness and response, in addition to addressing the known information security issues to achieve a state of management control as defined in the organization information security policies.

Comparing the action strategies undertaken in organization BETA against the piezoelectric behavior, it was clear that the control actions in organization BETA were a subset of the possible control actions in the piezoelectric theory to address known issues.

Similarly, the actions in the system of readiness and response devised, implemented, and executed in organization BETA to deal with emerging and new security incidents that were largely unknown to organization BETA were part of, or a subset of the possible action strategies in the system of readiness and response of the piezoelectric theory.

Given that the action strategies of organization BETA included both the actions for readiness and response, and control actions, it follows that the action strategies of organization BETA are part of or a sub-set of the action strategies possible of the piezoelectric theory of information security risk management.
In other words, what organization BETA has devised and implemented was in line with the piezoelectric theory of information security risk management, which showed that a responsive approach to manage both known and unknown security issues had made a difference in achieving a positive outcome, in particular, during an emerging incident.

The experience and learning from the readiness activities and responses implemented and executed in organization BETA supported the construct validity of the responsive approach, which also demonstrated how the focus on responsiveness was possible to address the risks of both known and unknown security issues in such an instance. They showed that when resources and focus were placed on a system of actions on readiness and response, the organization was able to manage the security incident more effectively and efficiently than in previous situations when such a system was not in place. As the incidents unfolded, we saw the enactment of the piezoelectric metaphor in real life, the alignment of individuals, groups, processes, and technologies in organization BETA that (unintentionally) assimilate to the electric charges within the piezoelectric material. This provides an important instance validating and supporting the efficacy of the responsive approach.

The differences in outcome, in terms of the impact experienced by organizations, including BETA, that were ready to act on the worm alert, security information, and patches available from BETA supported the claim that the organization that is not responsive to the adversaries’ behavior and actions, and related information risk events will more likely experiences a more severe impact than one that is more responsive.

In addition to supporting the validity of the responsive approach, the practices of organization BETA in its action strategies on readiness and response provided further insights on the specific actions that may be taken to implement such an approach in other organizations. They include:

1. Establish a structured organization of people, processes, and tools to be ready to respond to any unplanned events. The basic elements should include an updated contact list (for both internal and external key contact points); assigning individual responsibilities for security alert communication; and
establishing the appropriate tools for crisis communications, which may be emails, facsimiles, phones, and other suitable means.

2. Provide regular training and awareness briefings to all employees across the company.

3. Conduct drills to test the accuracy of the data (such as contact list) captured, and readiness of the employees to execute their individual roles based on the security situation involved. This triggered the idea of using scenario planning as one of the possible tools to enhance the readiness and responsiveness of all involved\textsuperscript{111}.

4. The need for a stand-down process when the incident is dissolving, which is elaborated further below.

A typical incident has three major stages of changes (from normal to critical and back to normal). As the level of significance of a security event increases over time, there are possible triggers along the timeline that signify the emergence of a security incident. Identifying and detecting these triggers are one of the critical steps to ensure effective and efficient response to the events, since the choices of actions available will diminish as the incident unfold (McGee, 2004, pp. 28-34).

At the same time, for every incident, it would eventually reach a “plateau” stage whereby the level of significance no longer rises over time. After this stage, the significance level would start to decrease. If individuals who responded to the incident remain at the same level of alertness (or “alignment”) state, it would be exerting undue stress on the individuals. Resources spent on facing the incident at this stage would be wasted if the incident is dissolving but everyone remained in the response position instead of getting back to their daily activities. Detecting the “de-trigger” is therefore another important step to allow for gradual and eventual stand-down of the people involved in the responses. This was one of the concerns expressed by the field teams in the subsidiary offices in organization BETA, in terms of the lack of communication of the incident standing down, putting them on high alerts longer than necessary.

On the other hand, if individuals stand down before the de-trigger was detected; the organization will run a risk of being unprepared again, with possibly a much higher
exposure since the level of significance of the event may be at its highest at that point in time.

An effective responsive approach therefore needs to cater for appropriate standing-down actions, with active monitoring of possible de-triggers, and strategies to ensure a smooth, but, not a false stand-down to normal condition.

4.4.3 Case Study B: Learning from the Tsunami incident

Disasters are often unpredictable. However, in terms of the Tsunami incident that happened in Dec 2004 (J20041226-1, J20061126), even though it came as a shock to most people, there were signals of its emergence hours before its occurrence. Despite the warning signals, countries who received them did not respond. Most countries assessed that the risk of Tsunamis as low, or insignificance, compared with other disasters that had strike before. This was in light of the well known disaster tragedies relating Tsunamis in Japan, and the preparation that Japan had since implemented.

The incident showed human’s tendency to assess risk based on past incidents in the local context, which tends to be biased towards local experiences. When there is no prior local experience, the risk would usually be assessed as low. This triangulates the observation and assertion made in Section 4.2.7, which highlighted the importance of making the subjectively assessed risks more explicit, bringing attention to the existence of risks that are largely unknown to the organization and the risk managers.

A change in strategy in information security risks in the era of constant changes and uncertainties is therefore also eminent.

While the absence of preparedness had cost the lives of many across the region, the fisherman’s experiences and the school pupil’s recall of geographical lessons on Tsunamis had saved many lives (BBC Online, 2005; Chin, 2004; Telegraph, 2005; UNESCAP, 2006). These positive outcomes illustrated the power of knowledge, strengthening the importance of situation awareness as one of the fundamental requirements to effective and efficient response. Again, the difference in outcome, to people around those who were responsive (like the fisherman and school pupil), and those who did not, were significant. This further supports the claim that the an organization that is not responsive to the adversaries’ behavior and actions, and related information risk events will more likely experiences a more severe impact than one that is more responsive.
4.4.4 Revealing uncertainties

An important step in managing uncertainties is to recognize that they exist, and disregarding them could result in dire consequences, as learned from the action research cycles and the analysis in Section 4.2.7. To gain recognition, the existence of unknowns must be made explicit, even though the unknowns would remain unknown. This would then provide a basis for management attention, discussion, and decision, before any action strategies can be devised and implemented. Drucker has, in essence, suggested a similar approach for managing risk to the business:

The main goal of a management science must be to enable business to take the right risk. Indeed, it must be to enable business to take greater risks—by providing knowledge and understanding of alternative risks and alternative expectations; by identifying the resources and efforts needed for desired results; by mobilizing energies for contribution; and by measuring results against expectations, thereby providing means for early correction of wrong or inadequate decisions (Drucker, 1990, pp. 511-512).

As discussed in Styles (2005), attention is closely integrated with perception, and most effective when visual perception is provided.

One possible representation of the unknown risks is through depicting a third plane (or axis) in the risk chart shown in Figure 27. By depicting the third-axis, it is clear that there are unknowns, and uncertainties in the risk assessments. The follow-up strategy for managing the risk will therefore have to address these concerns explicitly.

Figure 27: Element of uncertainty creating an invisible plane in the risk chart
A parallel of this issue of making the existence of the unknowns visible can be drawn from Hilary Lawson (2004)’s discourses on the notion of “saying the unsayable” when she questions the relationship between openness and closure.

The problem with the notion of ‘the world’ is that it makes it look as if the world lies already differentiated awaiting the descriptions of the language; as if the task of the human kind is to find the right description, the one that accurately names the bits of the world and their relationships; as if diligent scientists could uncover the ultimate building blocks of matter and we would know what the world is made of (Lawson, 2004, p. 284).

We can see this notion imposed on the risk managers in a similar manner, expecting them to be able to identify and assess all information security risks within the context of their organization and/or information systems comprehensively and accurately, given a set of methodology and tools—a form of closure.

Instead, I wish to propose that we hold the world as open. It is we who make sense of it through closure. We who, through the process of closure, hold openess as a complex array of things. Closure can be conceived therefore as a process that enables the flux of openness to be held as differentiated bits. Closure is the process of realizing identities, of realizing things. It is the mechanism by which we hold that which is different as one and the same (Lawson, 2004, p. 284).

The method in which common risk assessment was conducted further promote the ideal that all risks that need to be known can be known, only a matter of identifying, describing, and assessing their criticality.

The objects of science, the particles and laws, are not true descriptions of the world but are ways of holding openness, ways of making sense of openness so that we can intervene to effect. All of our sensations, all of our perceptions, all of our descriptions of the world are the product of closure and they have the characteristics of closure. They are not openness, nor do they have anything in common with openness (Lawson, 2004, p. 284).

The risk assessment method that we use therefore provides only a form of closure to the risk environment that allows us to intervene, but not necessarily represents the openness of the risk environment, since the risk environment is constantly changing. We therefore should not confine ourselves to a single closure.
At a simplistic level, the framework of openness and closure provides an explanation for our inability to describe the world. We cannot describe the world, because the world is open. Since openness has nothing in common with closure, if we pursue any individual closure, it is seen to fail. Each closure may offer a way of holding openness, but openness is something other (Lawson, 2004, p. 286).

The effectiveness of common approach in risk assessment has been questioned, and evidence from this study had illustrated its limitations, in particular, in dealing with emerging, and unplanned risk events. But, Lawson (2004, p. 287) adds that “failures do not tell us how the world is, but the manner of their failure tells us something about how the world is not.” The limitations of the risk assessment and management methods similarly did not provide information about the risk environment, but highlighted that the risk environment was not limited to what the tools and method assumed it to be. In other words, our analysis shows that the risk environment is more than what the common risk assessment method can address, that there is a difference between the worldview of the risk assessment method adopted, and the openness of the risk environment. The analysis triggers the idea of a third axis (a hidden plane that must be made visible), to provide another closure to the openness of the risk environment to allow for intervention. This is in line with Lawson’s theory of closure.

The strength of the theory is that it offers a description of how it is that although we are unable to describe openness we can nevertheless intervene in the world. It is this step that allows us to move on from the otherwise relentless circling of the self-reflective paradox (Lawson, 2004, p. 287).

In addition, Lawson asserts that:

Philosophy does not need to remain confined in the strategies of avoidance. We do not need to think that we should avoid the attempt to answer the questions that puzzle us most deeply. We do not need to conclude that because it is unsayable it should be avoided. For in some sense, everything is unsayable (Lawson, 2004, pp. 289-290).

The third axis, although contains the unknowns, should not be unsayable and must not be avoided. By making the third axis visible, we define a new closure to the openness of the risk environment. As Lawson stated, “Although each of these closures [may ultimately] fails in the limit, they are powerful nevertheless.” With this visibility, the closure is “capable of changing how we think and what we can achieve” (Lawson, 2004, p. 290).
4.4.5  Responsive, reactive, and proactive

Similar to the practices in organization BETA, analysis of the interviews and survey results from the 30 external practitioners showed that many organizations had indeed begun practicing information security risk management that were more responsive oriented, even though they continue to espouse a defensive-oriented strategy (J20061020). The external survey established that:

1. Security monitoring and disaster recovery were listed among the top three priorities in about one third of the responses. This reflects an actual practice that gave attention to preparedness (which was their theory-in-use). This was supported by the responses reported, in terms of their votes of the role of IT security function during the emergence and occurrence of a security incident, and in terms of their above average to high preparedness of the security staff for security incidents. The high emphasis on patch management (73%) and change management (67%) further showed that their actual practice was towards a responsive system of information security risk management.

2. The responses on the level of preparedness and the type of worms/viruses that caused major impact to the respondents’ organizations showed an inverse relationship between the two areas. That is, low preparedness resulting in higher impact when an unplanned or unknown security event emerged.

3. Conducting drills on security incident was not in the top three priorities of the security plan of any respondents. However, when security incident response was considered (even not as a top priority task), testing was performed by at least 47% of the respondents. A much higher state of preparedness therefore could be expected should the preparedness for security incident be considered as one of the top three priorities in the security plan.

This theory-in-use phenomenon can be explained as a defensive-oriented strategy that is generally perceived to be proactive—the notion of “prevention is better than cure”—projecting better control and leadership over the issues and concerns involved.

When the notion of a responsive security approach was first presented and discussed with other information security practitioners outside of organization ALPHA to seek disconfirming evidence, there were active discourses on the validity of the approach. As recorded in the research journal (J20050110), a few respondents were concerned
that such an approach will be too reactive, mistaken responsive for being “waiting for something to happen instead of dealing with information risk proactively.”

The responsive approach is however not a reactive approach. In the context of strategic management, Russell L. Ackoff identified three types of planning, namely “reactive”, “preactive”, and “interactive” planning as important for different needs, which would also influence the future of the organization and the environment that it operates in.

Reactive planning is bottom-up tactically oriented planning. What strategy it contains is implicit, a consequence of numerous independently made tactical decisions. It begins with the lowest or low-level units of an organization identifying the deficiencies and threats they face. Then they attempt to return to a preferred earlier state by designing projects intended to reveal the causes of these deficiencies and threats and to remove or suppress them. Next, using cost-benefit analyses, priorities are assigned to projects. Finally, using an estimate of the amount of resources that will be available for work on projects, a set of them is selected starting at the top of the priority list, working down until all the expected resources have been allocated. The set of projects thus selected constitutes the unit’s plan (Ackoff, 1999, p. 103).

Reactive planning is therefore issue-oriented, specific to what information security risk manager have been doing in response to auditors’ comments, and regulatory compliance requirements, and whenever a security breach occurred.

Preactive planning is top-down strategically oriented planning. Objectives are explicitly set but tactics are left to the discretion of individual units. Such planning has two parts, prediction and preparation, of which prediction is the more important. If a prediction is in error, even good preparation for what it predicts may be in vain.

The preactive planning process begins at the top of an organization with preparation of one or more forecasts of the future. These are analyzed for the threats and opportunities they present. Then a broad statement of overall organizational strategies for dealing with these threats and opportunities is prepared. The predicted future(s) and the strategic “white paper” are then passed down through the organization. Each level adjusts the forecast and the analysis to its own specific environmental conditions, and selects objectives and goals that are compatible with those of the organization as a whole. Programs to pursue these objectives and goals are formulated in general terms (Ackoff, 1999, pp. 104-105).
Information security risk managers who adopt a continuous risk assessment approach to determine new and emerging risk in response to organizational changes such as changing business systems and processes, and introduction of new information technology are in fact preactive in their planning. In general, this is often regarded as being proactive in anticipating issues before they arise.

Interactive planning is directed at gaining control of the future. It is based on the belief that an organization’s future depends at least as much on what it does between now and then as on what is done to it. Therefore, this type of planning consists of the design of a desirable future and the selection or invention of ways of bringing it about as closely as possible. (p. 106)

There are aspects of the future that we cannot anticipate; for example, natural or political catastrophes, or technological breakthroughs. We cannot prepare for these directly, but we can do so indirectly through responsiveness (interactive) planning. Such planning is directed toward designing an organization and a system for managing it that can quickly detect deviations from the expected and respond to them effectively. Hence responsiveness (interactive) planning consists of building responsiveness and flexibility into an organization. (p. 107)

A responsive approach is beyond being reactive and preactive. In line with Ackoff’s definition, it is future oriented, and more importantly, anticipatory of the unknowns and designing the organization and system to be responsive and flexible. Adopting a responsive approach in information security risk management is to ensure that the organization’s information security systems is future-oriented, capable of detecting deviation in the risk environment, and responding to them effectively. By preparing to respond, putting necessary processes and resources in place, practicing their use regularly, we become more alert to changing situations, and less reactive overall. The idea that being responsive is interactive, beyond preactive or proactive is important to also drive a positive perception for the piezoelectric theory.

It is also important to note that the responsive approach does not eliminate the existing practice of proactively resolving and addressing known security issues. Instead, it highlights the inadequacies and limitations in the preventive aspects, through escalating concerns on the issues relating to the lack of responsiveness of an organization. When an organization is only dealing with known issues, and expended all the resources available to only deal with known issues, as experienced in
organization ALPHA, the organization is often surprised by new or emerging security events. This caused the so-called “fire fighting” more than what the organization had anticipated.

### 4.4.6 Criticality alignment

The analysis in Section 4.2.7 on the information security risk analysis and management revealed that risk assessment is humanly subjective, filled with uncertainties and unknowns. An information security officer from a major financial institution participating in a security conference commented that “it is so subjective that we are just guessing all the time, and often not sure whether we are doing the right thing”, confirming my earlier analysis (J20061027). Another practitioner added that

> If we are to go through the entire organization to complete the risk assessment before taking actions to secure the systems, it will be too late, and we will never be effective. We need to have a basis to take actions to secure what’s most important for the business (J20061027).

If risk assessment is not practical for its subjectivity, and ineffective in addressing security issues, what alternative is available to information risk manager? Furthermore, given the constraints of business resources, and the primary focus of management, which is the business objectives, how do we gain the agreement and support of the business management to re-direct parts of those resources to risk management?

The situation is similar to those of business negotiation in which one or more conflicts of interest exist, even though there might still be recognition that information security risk needs to be managed.

According to Thomas Schelling’s classic work on “The Strategy of Conflicts”, in which such conflicting situations were discoursed, one possible strategy is to look for “prominent” solution that both parties could recognize. This would provide a focal point for establishing commitment (Schelling, 1960, p. 58).

This relates to the notion of criticality alignment, which is one of the three key stages of the piezoelectric behavioral metaphor. To recap, the proposition for criticality alignment is that:
A balance of focus from business can only be achieved if and only if information risk management is focused on criticality of the information risk to the business, and the mechanisms for managing risk have the ability to adapt to the criticality status of the systems and environmental, which varies with time and events in and around the systems ("Piezoelectric Metaphor", Section 4.4.1.)

The notion of criticality alignment defines and provides the focal point from which, the boundary of systems can then be identified, where business interest and risk issues intersect. Based on the principles of piezoelectric analyzed in the earlier research cycles, criticality alignment was identified as the area where information risk manager should focus in order to be aligned with the business needs, and responsive to issues emerging from changes in the organization systems and environment. This extends the notion of criticality used in other existing approaches, such as the “materiality” of risk in Knowles (2005), and the criticality of risk in organization BETA, which only provide an indicator of the importance of an asset involved. Alignment relates to outcome. Together, the notion of criticality alignment means something that need to be acted upon to result in desired outcomes. Criticality alignment is business directed and business aligned, focusing on business undertakings, which may be a project, an initiative, a program, an uncertainty of concern, or something that has a significant effect on a business, and therefore management must act. Using Flood’s (1999) Four-window systems view, organization may also include fairness as one of the desired attributes, or requirements for criticality alignment.

The criticality alignment of the business consists of two groups of issues. One is the intersections (or overlaps) between the business critical concerns and the results of a risk assessment. The other is the business concerns that are not surfaced in the risk assessment. For example, regulatory compliance is often a business concern, but from an information security risk assessment perspective, it is not considered an information risk, but rather a regulatory risk (from an overall business risk perspective.) Through the process of identifying and assessing criticality alignment requirements, regulatory compliance would therefore surface as one of the concerns requiring focus by the information risk managers.

Regulatory compliance, however, is not the only critical alignment. In the external survey conducted, business continuity was rated as the top reason for implementing information security, with 22% of responses, 3% higher than regulatory compliance.
One reason for regulatory compliance to be placed as a low priority relates to the nature of the industry where the organization operates. For example, in a security workshop conducted with a telecommunication company in Indonesia, the IT manager reported that there was no regulation (at the point of this writing) that mandate any information security management and practices in the country. As such, in their context, regulatory compliance is not a driver for implementing information security risk management (J20061108).

As the business environment is constantly changing, so as the risk environment, the criticality alignment requirements of the organization are therefore not a constant, and must not be regarded as such. The method of discovering and affirming the criticality alignment needs of the organization should therefore allow for changes and outcome from the initial process be reflected and considered to trigger the next round of evaluation and action strategies. An action research approach that is dialectic and iterative is therefore preferred over a static process. The dialectic variation (Dick, 2002f) of the Soft Systems methodology (SSM) (Checkland & Scholes, 1990; Sankaran, Tay, & Cheah, 2004) was adopted for this requirement. The SSM-based dialectic approach also provides added benefit through the introduction of the ideal world model to compare with the essence of the existing environment, allowing the participants and researcher to gain more clarity through the comparison before determining where improvements should be focused upon.

The approach of using criticality alignment as the focal point for justifying information security systems in organizations was also found to be more acceptable from the business perspective, as reflected in an interview with the CIO of a multi-national logistic company in Singapore (J20030401). As noted in my journal,

> The focus [of the logistic company] is on using IT to automate more of their business processes and create more value to the business, and implementing information security, if it is part of the product/systems that they get without paying, they will do it. Otherwise, they will have to consider hard. (J20030401)

When discussed with a group of senior government officials involved in promoting information security practices in the industry in 2003, as recorded in my research journal,

> I highlighted the concept of criticality alignment, emphasizing the need to influence people’s mindset to focus on what is really critical to their business, and what critical
events that they must manage and stay “alive”, such that if they integrate information security with those services and events, then the values of information security would be specific, and users and management would then be aligned and committed to implement good practices in their organization. By doing this, they would also align the information security policy, processes, tools, and procedure to focus only on getting prepared for critical events, and delivering critical services reliably, instead of across-the-board controls and security, which digress users and management attentions and resources.

The group deliberated on this concept, and affirmed that it is a fresh approach that they have not come across before. They felt that it could make sense. However, since it is so new, there would be barriers for them to implement. Borrowing the concept, the group realized that they could perhaps achieve their objective [of promoting information security as a key lever in the country] if they focus on a segment of the industry, those that provide critical services to the Financial Industry and Government, then perhaps the target is more achievable, since the demands for security will be more direct from the service acquirers, whom themselves need the information security assurance for their business. The [group] was satisfied with this conclusion and seemed determined to bring this to fruition. (J20030401)

As a result of the discussion, the government department decided to fund the development of a new IT standard for business continuity and disaster recovery services provider, after further assessment in which its criticality alignment was strongly recognized. I was the chairperson for the IT Security Standards Technical Committee that assisted in the process and supported the development of the new standard. The standard was completed in 2004 and published as a national IT standard—SS507, “Singapore Standard for Business Continuity/Disaster Recover (BC/DR) Service Providers” (SPRING Singapore, 2004).

The BC/DR standard development provided two important outcomes for this study. The first outcome relates to the understanding and acceptance of the concept of criticality alignment, which was highly positive, as illustrated by the subsequent actions taken by the government. More important to this study is the second outcome, which brought the government official to focus on a critical area for the businesses, and the IT environment in the country, which has a positive influence on the perception of Singapore as a “Trusted Hub” for the Asia region, leveraging its advantage of an earthquake-free geography, and strong IT infrastructure. The SS507
standard was first of its kind in the world, and in April 2005, was submitted to the International Standards Organization (ISO) and accepted for further development to evolve into an international standard. The concept of criticality alignment has therefore helped to deliver an important outcome, demonstrating its validity as a principle to create alignment with the business, by focusing on the critical alignment requirements and action strategy in terms of information security needs, and the business (in this case, the government) desired outcome.

Given the efficacy of the approach of using criticality alignment in this study to gain stakeholders agreements and identify focus for information security risk management, it appeared that the notion of risk assessment is redundant. This is, however, disconfirmed as a valid proposition. Risk analysis and assessment are still relevant and necessary, even though they are humanly subjective. Risk assessment forms part of the criticality alignment identification process. Risk assessment provides the required list of known and perceived risks. The human subjective part of risk assessment may be discounted, but the list of risk items identified provides a logical and rational basis for approaching the stakeholders to reach a consensus on the criticality alignment requirements of the organizations. Without the list of risk items, the stakeholders would not have realized that many of those information security risks exist, and how they relate to the business. It would therefore be impossible to identify the criticality alignment needs that include those risks that are of concerns to the information security risk managers. Through this study, we introduced the concept of criticality alignment, and the third-axis to complement for the inadequacies of conventional risk assessment approach. This contributes to the knowledge domain of information risk management.

4.4.7 Ecological validity – Testing the responsive approach in organization CHARLIE

An opportunity to implement and test the validity of the responsive approach arose when I worked with the chief security officer (CSO) of organization CHARLIE, a retail bank in Thailand. The responsive approach for information security risk management presented a new perspective for addressing the challenges of managing information security risk in organization CHARLIE, which was faced with a series of virus and worm programs attacks resulting in significant business losses (J20050711).
Using the SSM-based Dialectic Model of Systems Inquiry (DMSI) and the IRM framework (see Appendix D), I worked with the CSO of CHARLIE to devise a new security infrastructure and systems to address both existing (known) risk issues, and plan for future requirements, based on the CIO’s vision and plans, and the criticality alignment needs of the organization (J20061126). Execution of the DMSI for the testing is described in Section 3.3.3.3.

The implementation in organization CHARLIE observed another limitation about existing risk assessment methodologies such as OCTAVE (Alberts & Dorofee, 2002), ISO/IEC 13335 (ISO/IEC, 2004, 2005a), and various commercial methodologies, as also described in Moses (1994), that most consultants as well as organization CHARLIE were using. There was an assumption in those methodologies that a system already exists such that the risk assessment was about identifying risks relating to that system. When a new system was desired, where there was no existing system to be used as a basis for risk assessment, those methods became inadequate. Information security officers or risk managers would then have to wait for the information system designers to complete at least a first draft of their system design before they can conduct a risk assessment of the draft system. This posited risk management as a reactive step to the design, requiring changes to be made thereafter when the risks of the original design have been identified, assessed and analyzed. On the other hand, what the CIO wanted from the CSO was a set of security recommendations, including requirements and action strategies that should be considered or mandated as part of the new infrastructure and information systems design process. This could then result in a new systems design that has the security needs integrated and provided as part of the system. This prompted the search for an alternative methodology, which resulted in the development of the IRM framework (see Figure 35, Appendix D), based on previous work that was completed for capturing similar requirements for use in the standards development area—another iterative development of the original framework.

The IRM framework and the SSM-based DMSI enabled the information security team to sieve through many aspects of the organization to identify the key requirements, the essence and ideal of those requirements, the actual and practical implementation that were feasible, to derive the five-level action map (FLAM). The outcome of the FLAM was a comprehensive security plan that addressed the known security risks and key requirements, as well as serve as a foundation for the CSO to build a more responsive
system for preparing against the unknown and unexpected security issues that would likely emerge thereafter.

The use of the concept of criticality alignment was able to identify and align the critical business needs (of the CIO and business managers) to the IT security concerns and bring about common focus and therefore secured the necessary resources to implement the security plan. Unlike traditional security plans that addressed only the known (or identifiable) risks, with minimum or no preparation to deal with the unknowns or unexpected, the new security plan devised and implemented in organization CHARLIE had catered for the response needs so that the organization can become more responsive to upcoming changes that were planned for the organization, as well as unexpected changes that would emerge from the planned changes and other changes in the risk environment (J20061126).

As described in Section 3.3.3.3, the final dialectics in the implementation involved evaluating the results of the external security tests conducted on the new security infrastructure that was designed based on the responsive approach, focusing on the vulnerability management system, which addressed known risk issues, and the security updating system, which addresses a critical range of newly known issues. While a dynamic performance monitoring and measurement system was not implemented in this test (which was not feasible due to resource constraints both on the research study, and the testing organization involved) to provide a measurement of the responsiveness of the organization, the security readiness of CHARLIE reflected its state of responsiveness. The security readiness of CHARLIE was demonstrated by the following:

a. The new IT infrastructure has incorporated the component systems required of a responsive approach, namely, a system for distributing and installing security updates and malware signature updates as and when those updates have been made available by the providers and approved for deployment by the CSO’s security operation staff member.

b. CHARLIE has implemented a process that keep tracks of occurring events and a team of operation staff to evaluate those events and get ready to respond should they become a security incident. The process
was further supported by the implementation of an incident response and handling procedure. The operational staff members were trained on the operation of the new IT security systems as well as the event monitoring and incident response procedures.

c. CHARLIE engaged a third party security consulting service company to conduct a security penetration (attack) test. The objective of the test was to ascertain that the organization’s IT infrastructure was able to withstand organized attack by external perpetrator, using known vulnerabilities commonly found on IT systems and applications. CHARLIE passed the test conducted by the third party, which established that the new security infrastructure in organization CHARLIE was up-to-date with security patches and anti-malware signature, and the operation of the IT infrastructure did not provide weaknesses for commonly known attacks to perpetrate successfully.

With the above IT systems, process, and testing conducted, CHARLIE has the necessary infrastructure systems and processes in place and was tested ready to respond to both known risk issues that it was designed to address, and the critical range of newly discovered issues that it was developed in preparation for the updating needed, which therefore showed that CHARLIE was now more responsive than it was before the implementation of the responsive approach.

As discussed in Section 3.2.1, an important quality criterion for evaluating the outcome of the research is the concept of ecological validity, which is concerned with the extent to which it is possible to generalize from the actual social context in which the research has taken place and data thereby gathered, to other contexts and settings (Gill & Johnson, 2002). In this regards, the outcome of the implementation (as described in Section 3.3.3.3, with the results analyzed and interpreted above) in organization CHARLIE has provided data to support the ecological validity of the responsive approach, illustrating how the responsive approach that emerged from the social practice context and data gathered in organization ALPHA and BETA may be generalized for application in organizations such as CHARLIE, and was ecologically valid in CHARLIE, which has a different social and practice context.
The validity of the responsive approach for information security risk management was further triangulated with the feedback received from a group of practicing information security officers (J20050915, J20070219), and two other senior information security practitioners, who separately found its applicability in their respective organizational context. In a review conducted by a CSO of a regional bank in Singapore, the senior practitioner commented that:

> Your attempt to [use a framework to] dissect it into various levels to make it comprehensive and goes down as far as possible to guide potential implementers is good.

For most of us who have been in the industry for a while, these are things that shape all of our decisions and actions. I would say that we are all looking at these areas for our day to day activities. Different environments may have different approaches but overall, what is in the paper holds true. (J20060108)

According to a senior regional information risk manager who studied the approach and separately tested the concept in her organization’s practice:

> The organization is now increasingly focused on monitoring systems and applications reliability and availability, and also how fast the development teams and IT functions can response to an incident. This was started subsequent to a massive business application failure resulting in substantial losses to the organization. Since then, bi-weekly review of systems and applications performance have been taking place. An important development in this area is that she (the regional IRM) has been involved in this initiative, introducing the responsive approach, and looked upon as an entity that can help to improve the risk status and profile of the applications involved. By focusing on the responsiveness, they [the application development teams] have improved application uptimes by multiple folds, and reduced the time it took the development teams and IT to fix a new problem. This was achieved also thru’ breaking down the measurement of the time-to-fix to individual application team rather than a total system measurement. The approach reaped the benefit of making every team focus on its part in reducing the time-to-fix and improving the quality of their work to improve the uptime of their respective areas (J20060717).
4.4.8 Case Study C: Learning from the Antinny worm case study

Two key learnings emerged from studying and reviewing the Antinny (Microsoft Corporation, 2006c; Sophos Plc., 2006; Symantec, 2004a) worm incident which emerged in April 2004 (J20061126). The incident showed the state of lack of preparedness, or readiness to respond to security incident, both emerging and occurred, amongst the Internet Services Providers (ISP) community in 2004 in Japan, even though there were already numerous security incidents involving network worms and denial of services attacks in and before that period; for example, see CERT/CC (2003b), Legon (2004), Lemos (2004), Microsoft Corporation (2004), Pelline (2004), Symantec (2004b), and US-CERT (2004a; US-CERT, 2004b).

The dilemma was that there was also not a lack of support or sponsorship from key stakeholders involved, as shown by the creation of the Japan Telecom-ISAC program in early 2004, which signified their awareness and commitment to address such security risks on the Internet. The focus of the Japan Telecom-ISAC program was however on monitoring and detection, and after-incident reactive measures, instead of how the community should respond to emerging security incidents. The ignorance of the principles of piezoelectric and the importance of responsiveness is attributed to such a design of the Telecom-ISAC program. Consequently, the attack was able to continue for a prolonged period, even though the incident had already been detected. In the concluding remarks, asserting the lesson learnt from the incident, Nakao (2006) therefore recommended the implementation of “measure for evasion, against DDoS attack”, and capability to “predict and foresee, so that [responsive] controls can be deployed in the early stage [before the occurrence of an incident]” (Nakao, 2006).

Another important learning from the Antinny worm incident relates to the availability of technology that was ready for deployment to provide for the responsive needs of the ISPs. In this case, the Sinkhole (Mirkovic, Dietrich, Dittrich, & Reiher, 2005, pp. 175-178, p. 175-178) networking approach was developed a few years back when denial of services attack was assessed to be a significant threat for businesses operating on the Internet. However, its adoption has been limited since it does not serve a useful purpose in normal operating conditions. The principle of piezoelectric is therefore important from a strategic planning perspective, which signifies the need for responsive technological infrastructure to manage the changing IT risk.
environment, instead of justifying such investment based on a risk-based only approach, in which the non-occurrence of DDoS in the past would result in a tendency for such an attack to be assessed as a low risk event to the organization.

Besides the Sinkhole network, in response to the threats of Internet attacks, a number of security technology and concepts aimed at providing better capability for detecting and identifying new and emerging attacks, in particular, those that are using new techniques and exploiting not publicly known or reported vulnerabilities have also been developed in the recent years. For example, Honeypot (Amoroso, 1999, pp. 169-184; Takakura, 2006; The Honeynet Project, 2002, pp. 9-12), HoneyNet (The Honeynet Project, 2002), Strider HoneyMonkey (Y.-M. Wang, Beck, Jiang, & Roussev, 2005), and Darknet monitoring (Bailey, Cooke, Jahanian, Nazario, & Watson, 2004; Bailey et al., 2005) are some of the security technology and concepts in which their use could provide the necessary technical capabilities to improve an organization’s responsiveness to new attacks on the Internet.

While the responsive approach for information security risk management was not the basis for the development of these responsive security technologies, the nature of these technologies, in terms of their design and deployment, have all converged towards providing for better detective capability that would improve the responsiveness of the organizations using them. To justify their adoption and deployment, the use of the responsive approach, promoting a responsive strategy for managing information security risk in the organization is therefore in order.

The emergence of responsiveness from the application of the responsive security technologies further illustrated the construct validity of the responsive approach. In other words, the outcome of the responsive security technologies contributes further to the responsive approach in defining the technology elements and processes for improving security readiness, and hence, responsiveness.

### 4.4.9 Refining the responsive approach

With the understanding on the limitations of common risk assessment method such as the ISRA method used in organization ALPHA, and the conclusion that a third axis on the unknown risks need to be made explicit to increase awareness of the risks, the question was how should this be implemented in the practice environment.
4.4.9.1 Risk forecasting

As the risks are unknown to the risk manager, it would be impossible to reflect them graphically at the third axis (Figure 27). Given the complexity of the organizational systems and environment involved, as Flood highlighted, advanced planning would not be feasible to deal with the unknowable:

> Complexity theory questions whether long term intended action is possible. It points out that the way things unfold is inherently unknowable to the human mind, emerging through spontaneous self-organization originating from some distant detail, rather than advanced planning. The most we can do is to manage what is local, whilst appreciating the incomprehensibility of global complexity. Managing what is local entails continually considering outcomes that extend over a small number of interrelationships, very few stages of emergence, over only short periods of time into the future. This is what I meant by learning within the unknowable. We learn our way into a mysterious future (Flood, 1999, p. 90).

In other words, to be meaningful to the risk manager, business management, and individuals in organizations, like the meteorologists in weather forecasting, the third-axis should reflect the risk forecast for the organization. Like weather forecast, the risk information could then be used for determining suitable responses and action strategies.

Open systems theory states that all systems have permeable boundaries and are, therefore, open to their environments. Some systems may also have relevant “task environment,” one lying between the social environment and the system. For a system to be viable over time, it needs to (1) constantly scan the relevant environments for changes that might affect its viability; and (2) actively adapt to new information it receives in such a way that it also influences those environment (Emery & Devane, 1999). Such sources provide useful information for the risk forecast required for the third axis.

The analysis of information security risk management as a system in organization ALPHA showed that it has causal behaviors similar to open systems. In order to deal with changes within, and also external to the system effectively, we need to design and implement attributes that enable it to detect relevant changes in the environments, and actively adapt to the new information it receives in such a way that it also influences those environment. Traditional approaches implement monitoring systems
to focus mainly on past event records, things that have already taken place in the system, instead of looking for emerging changes in the environment. As such, incident response, disaster recovery, and business continuity management elements often focus on recovery and investigation instead of changing the protection systems in response to the external changes detected or identified\textsuperscript{117}.

Implementing and managing information security risk in an organization needs to deal with changes within as well as external to the organization. These changes have peculiar characteristics that are at times similar, but could also be different than other organization changes that are often initiated by the business, or instigated by the external changes where the organization exists. The methodology employed as part of managing information security risk should therefore be ready to deal with those challenges similar to common change management while cater for the needs or requirements of information security in the organization.

To forecast risk, knowing and understanding those changes are fundamental. This requires close monitoring and observation of the operational status of critical parameters in or affecting the security of existing systems and environment, not just learning from past events, but also new events and their emerging characteristics, and linking them to the critical alignment needs of the organization. This may also include risk forecast available from external sources on the Internet. For examples, the “Internet Storm Center” operated by the SANS Institute\textsuperscript{118}, the University of Michigan’s Internet Motion Sensor (Bailey et al., 2004), and other organization groups such as the Japan Telecom-ISAC Internet monitoring initiative (Nakao, 2004, 2005).
Ideally, the likelihood of an adverse event occurring should be projected by assessing the current status against past known events that have similar patterns of behavior, or attributes. However, unless an extensive database of past security events is available and appropriately coded to permit real time pattern matching with ongoing developments, this estimation of probability of adverse event in real time is not be possible (Blakley et al., 2001). Such a system will also be context dependent in order to be relevant to the organization’s information security environment. In practice, such database will be costly to build and maintain.

Based on what we can find and access more practically from both internal and external information sources in the existing context, there are at least four categories of information that could potentially be tapped to provide for the purpose of information risk forecasting (Figure 28):

1. Technology (including products and applications) vulnerabilities and attacks data that is available from external sources, including security and updates (patch) advisories, patterns of network traffics and latest viruses/worms detected in the public domain, such as those reported by SANS Institute\textsuperscript{119} and the Telecom-ISAC (Nakao, 2004, 2005) as highlighted earlier;

**Figure 28: Sources of information for Information Risk Forecasting**
2. Internal and edge (perimeter) network security monitoring system, based on systems and security logs captured and reviewed by the intrusion detection systems;

3. Internal systems and applications failures data (including security and non-security related failures), available from both IT and applications teams. Incident reviews of failure events, in particular, unexpected events, should be conducted frequently and soon after something unexpected occurs, so that memory of the event is captured when peoples involved are fresh from it, and also diminishing opportunity for people to revise their stories in their attempt to show that they have taken the appropriate actions, therefore relinquishing responsibilities\(^{120}\) (Weick & Sutcliffe, 2001, p. 66); and

4. Human resource related data, such as new hires and employees leaving, contractors on-boarding or off-boarding, visitors’ profiles and access frequencies, and records of disgruntled or potentially disgruntle employees. All this could serve as indicators of the risk profile relating to people in the organization.

For a start, instead of plotting graphs for presentation purposes, a list of emerging issues, including statistics and trends in these four areas could be developed to provide a view of the potential risks ahead (a forecast \textit{per se}.). The individual items in this list can then be traced to see if they match any of the criticality alignments required by the organizations, as shown in Figure 29. From this we will get a list of key risk indicators (KRI), which have a clear match from the emerging risk to the requirements for criticality alignment (RCA), and a list of residual and systemic risks, which are not directly matched to any specific needs.

When there is a match, an action strategy may be devised to prepare a response for the emerging risk being forecast. However, the action strategy will have to be accepted by the management in order to gain their support and commitment. Techniques that have been tested effective in the social-technical approach (for example, SECD4 model as shown in Figure 22) can be applied to achieve this desired outcome. The basis for the action strategy must also be valid and based on sound principles and accurate data.
4.4.9.2 Scenarios planning and development

As the responsive approach is about addressing the unknowns, there are lessons that we can draw from related literatures in the organization and business management domain, even though there is no information security risk management specific literature in this area at this juncture.

Figure 29: Mapping Risk Forecasts against Requirements for Criticality Alignment

In analyzing the history of systems failures, Paul Ormerod (2005) concluded that, ultimately, all systems will fail one way or another. However, Ormerod rationalized that:

No biological species, with the exception of humanity, is able to anticipate the future and to plan its strategy accordingly. In reality, extinction is a pervasive feature for biological species, as it is for firms. Yet the people in companies are able to think about strategy, they are able to make decisions which will affect the ability of the firm to survive, and still extinction is an evasive feature (Ormerod, 2005, pp. 186-187).

As such, if we can identify potential failure situations early or in a timely manner, actions can then be devised to at least try to prevent the failure from taking place. In the worst case, even when the failure cannot be avoided, we can still prepare for survival in those situations.

We have encountered many examples of situations in which it is extremely difficult to penetrate the curtain of uncertainty which shrouds the future. From simple games to more complicated ones like chess to the real-life world of decision-making in business and politics, no matter how carefully researched and planned, the future
consequences of decisions made today are frequently surprising. To have the intention of securing a particular outcome is usually no guarantee at all that it will be achieved. Intent is not the same as outcome (Ormerod, 2005, pp. 186-187).

Although the intention may be different than the outcome, intention will drive actions and affect readiness, and affect the outcome. If there is no action, then we will be leaving everything to run its own course. This is certainly waiting for disaster to happen, which is undesirable. The readiness of the organization will make a difference when a disastrous situation arises.

In his final remarks, Ormerod asserted that “knowledge and innovation are the keys to survival, to prolong the period to extinction”. On dealing with the unknowable in complex organization, Ralph D. Stacey also commented that:

The long-term future of an innovative organization is unknowable: it cannot be predicted to any useful extent. This follows from what scientists have discovered about nonlinear feedback systems, of which a business organization is one. The unpredictability arises from the very structure of the business system, not simply from changes in markets and technology (Stacey, 1992, p. 13).

To deal with the dynamics of complex organization, and the unpredictability and unknowns, Stacey suggested:

Innovation and new strategic directions, however, require the development of new mental models—new maps—for new situation. In other words, no person, no book, can prescribe systems, rules, policies, or methods that dependably will lead to success in innovative organizations. All managers can do is establish the conditions that enable groups of people to learn in each new situation what approaches are effective in handling it. There cannot be comprehensive installation, only piecemeal intervention at sensitive points in the system (Stacey, 1992, pp. 15-16).

This raises the question of how do we develop the required mental model if people in the organization have no prior experiences in security incidents or related situations? As learned from the Tsunami incident (J20041226-1, J20061126) as discussed in Section 4.4.3, the young pupils and fisherman who saved many lives at the emergence of the incident were able to relate what they learned previously and use that knowledge to make a difference. What they knew about Tsunami was not completely similar to the actual event. But the knowledge of it enabled them to relate and response. Such kind of knowledge is most useful, even though it was not a perfect
match to the situation, and will never be. This form of knowledge, when available, is like providing an “imaginative leap into the future”, similar to the concept of scenarios planning as promulgated by Peter Schwartz and his colleagues (Schwartz, 1996). According to Schwartz,

Scenarios are not predictions. It is simply not possible to predict the future with certainty… Rather, scenarios are vehicles for helping people learn. Unlike traditional business forecasting or market research, they present alternative images of the future; they do not merely extrapolate the trends of the present.

Scenarios allow a manager to say, “I am prepared for whatever happens.” It is this ability to act with a knowledgeable sense of risk and reward that separates both the business executive and the wise individual from a bureaucrat or a gambler (Schwartz, 1996, p. 6)

The scenario-based training system, as described in Tay & Lim (2004) and analyzed as part of this study (J20061126), provides additional insights on the use of scenarios, and how it could affect the level of awareness and competencies. Although the scenario-based training system project was not about information security risk management, the problem situation was similar. The customer services officers were required to respond to incident situations in which they may not have direct or prior experiences, and the use of traditional classroom training was found to be ineffective. Similarly, individuals in organizations are required to respond to security incidents, many of which have no direct or prior experiences. Evidence from the case studies (in Sections 4.4.2, 4.4.3 and 4.4.8) showed that:

1. The level of responsiveness has a direct co-relation with the level of awareness and competencies. To improve responsiveness, we need to improve the awareness and competencies of the individuals;

2. Scenarios provide a proven method to improve awareness and competencies;

3. In situations that are impractical to conduct scenario drills using the actual environment, as in the North-East Line mass rapid transport system (Tay & Lim, 2004), technical simulation systems may be applied to improve learning and achieve better awareness and competencies;

A method suitable for improving responsiveness to information security risks in an organization is therefore to identify relevant security scenarios that may have critical
effects to the organization, i.e., requiring criticality alignments when such similar scenarios materialize.

Security scenarios may be built from knowledge of incidents of failures and attacks, both inside and outside the organization, as well as from analysis of attack trends, technology, business, and social trends and changes. Research reports on these subject matters, for example, the work of Kienzle and Elder (2003) may also be used to ensure that the scenarios are realistic and relevant to the organization. Heijden (1996, pp. 183-224, p. 183-224), Ringland (1998; 2002), and Schwartz (1996, pp. 241-248, p. 241-248), for examples, have provided useful teachings and insights for developing scenarios and using them in the strategic planning process.

However, this tactic for improving responsiveness only addresses the people aspect of managing information security risk. Organization information security is also affected by technology implementation – in infrastructure and application systems – and processes that operate and support them. Integrating responsiveness in technology and processes is therefore also desired.

From the technological perspective, in addition to the SBTS (Tay & Lim, 2004) and analysis of the Antinny Worm incident (Section 4.4.8), numerous technology advancements in networking and security are in fact progressing towards providing for responsiveness. The Sinkhole network has no purposeful use in the normal operation situation, but becomes valuable when a denial of service attack emerges on the network. Use of the Sinkhole therefore provides for responsiveness to such attack. Similarly, the concepts of “network isolation” (Chapple, 2007; S. Clark et al., 2006), and “segmentation” (Fernando, 2002; Norton, 2001) provide for the ease of segregating networks into applications or services zones so that attacks or technical problems emerging on a specific or group of related applications or services can be contained and not affect those in other network zones, enabling the organization to focus its responses to the affected zones and continue its business in other areas accordingly. To design and implement suitable technology infrastructure, understanding of plausible risk scenarios is again fundamental. Investing in technology readiness provisions will otherwise be unjustifiable.
4.4.9.3 Responsiveness requirements and action strategies

Knowledge of the key risk indicators (KRI), residual and systemic risks, and security scenarios collectively results in the organization’s responsiveness requirements. These requirements provide useful input to determine the action strategies necessary to improve resilience and responsiveness of the organization. In addition, a set of assurance action strategies is required to track progress, establish the state of readiness, and ultimately gain confidence of the ability of the organization to respond effectively and reliably to the next unknown information security event. These action strategies may be considered and developed using the FLAM planning framework derived in action research cycle 2, as depicted in Figure 21 (J20060719). These collective actions, as shown in Figure 30, define a system model for implementing the responsive approach for information security risk management.

Figure 30: An information risk management system model based on the responsive approach for information risk management

Note also in the system model (Figure 30) that the action strategies are implemented through two final components, i.e., the policies and program.
4.4.9.3.1 Information security policies

On policies, it is important to note that a responsive approach to managing information security does not preclude the formulation of policies or rules of operations in the organization. A responsive approach does not mean that organization should or can stop developing and implementing controls in view of known security risks or issues that can be addressed by those controls. On the contrary, rules and policies are critical in providing for responsiveness, and such an approach requires the identification and formulation of rules and policies, and resulting control measures, to be more rigorous, so that they should be structured to permit responsiveness rather than stifling it. As discussed by Malcolm Gladwell (2005) on the notion of “thinking without thinking”, rules form an important foundation for competitive games players and artists to be able to respond effectively and efficiently during a competitive or highly stressed situation, in which the situation cannot be completely simulated or rehearsed as it is. With rules and practices, the players and artists are able to learn their individual and corresponding roles and responsibilities, understand the strengths and weaknesses of individual players and artists, and have opportunities to expose themselves to many near similar practice-made scenarios. These also provide them with the opportunity to polish their skills to respond effectively and efficiently to the changing environment. At certain point, the players and artists can then proclaim their state of readiness or preparedness to deal with the uncertainties of an actual competition and live performance (Gladwell, 2005, pp. 114-120).

4.4.9.3.2 Information security program

The information security program forms another critical component for implementing the action strategies, designing suitable activities for improving protection, responsiveness, and assurance, within the bounds of the laws and regulations, and information security policies and rules.

The information security program should therefore consist of at least three components. One is the program for addressing the known risks, as in the improved IRM program (Model A) implemented in organization ALPHA. Through this research, the devised IRM framework (FIRM) as depicted in Figure 35 combined with the five-level action map as depicted in Figure 21 and the dialectic model (Figure 8) discussed
in Section 3.3.3.3 have been validated to produce reasonable outcomes (see Sections 4.3.5 and 4.4.7; also detailed in J20061126).

The next component is to plan and be prepared for the unknown risks, which is the implementation of the processes and technology, developing the security scenarios, and training the people in the organization to materialize the system model as depicted in Figure 30, up to stage of the action strategies formulation. Based on the security scenarios, conducts regular drills to train and test the readiness of individuals and groups in the organization.

The third component of the information security program is to support the assurance action strategies. As noted earlier, this involves tracking of progress in the other two components of the program, establish the state of readiness, and assess the level of confidence of ability of the organization to respond effectively and reliably to the next unknown information security event. This component provides the performance indicators, replacing the scorecard system that was used in the “Model A Approach”, which was found to be ineffective and unreliable.

4.4.9.3.3 Readiness assurance

The response readiness assessment in the assurance component provides two important indicators to the management and stakeholders. One is the state of readiness of the information infrastructure for knowing about potential information security risks that could impact the critical information assets of the organization. This includes the operational status of the monitoring systems highlighted in Figure 28, and the sub-system for identifying and tracking the requirements for criticality alignment of the organization in Figure 29. Next, based on the set of security scenarios that are applicable to those risks forecasts, how prepared are the organization, including technology, processes, and people, to respond to the materialization of those risk scenarios (Figure 30). The state of preparedness may be measured in several levels, such as, resources readiness, and measurable outcome during testing and drills over the scenarios over a series of tests and drills conducted.

4.4.10 Responsive learning

The initial study on the issues and dilemmas of IRM in organization ALPHA, as described in Section 4.2, revealed that the Model I, single-loop learning, behavioral
model was predominant in the organization. Policies compliance, risk mitigation, and controls orientation, with zero risk tolerance and no questioning of the governing variables against the consequences of the risk management actions, were observed as a common theme of the initial action research cycles. As Argyris and Schon commented:

Under conditions of little public testing of assumptions, low risk-taking, and the resulting high probability of self-sealing processes, we believe there will be little attempt to question the governing variables of model I. The learning behavior according to model I encourages learning that preserves the governing variables of model I and the behavioral world generated by model I; this is single-loop rather than double-loop learning (Argyris & Schon, 1991b, p. 79).

To bring about double-loop learning, a social-technical approach to managing information security risk was desired. Through the initial action research cycles (1 and 2), a revised approach incorporating five key elements, namely, stakeholder (S), entry and contracting processes (E), convergent interviewing (C), dialectic data analysis (D), and Flood’s Four-window view (4), i.e., SECD4, was developed, enhancing and evolving from the initial approach that was devised as part of the initial research cycle (Figure 22, Section 4.3.1.5).

![Figure 31: Argyris and Schon's (1991b) Concept of Single and Double Loop Learning](image)

In the course of the research, through the series of security incidents, we observed and reflected the limitations of the SECD4 social-technical approach. Although the social-technical approach was able to address stakeholders’ concerns and influences, the responsiveness of the organization to emerging and new risk issues remained a major constraint to managing information security risk. This led the research to the development of the responsive approach for information security risk management (Figure 30).

From a macro perspective, comparing the model for the responsive approach (Figure 30) to Argyris and Schon’s single- and double-loop learning model (Figure 31), it
emerged from Figure 32 that the governing variables and action strategies has become inherent in the responsive approach, with the outcome of one influencing the input and outcome of the other.

As responsiveness is a key element in this model, data sources such as those depicted in Figure 32 provide relevant information and intelligence about the changing risk environment and situation. These data sources form a key component of the model. Those information and intelligence relating to changing situations are posited to check against the governing variables, and further used in developing and evolving the action strategies, in addition to evaluating the consequences of those strategies.

As illustrated in Figure 32, the changing situation within and external to the organization serves as part of the inputs, and evaluated against the governing variables for determining the information security and responsiveness requirements for updating the action strategies. Similarly, execution of the action strategies will result in changes in the organization systems, as part of the outcome, or consequences. Those consequences are not necessarily the sole product of the action strategies. Ongoing changes in the organization systems and environment, including peoples’ behaviors, will continuously affect the system’s (including, again, people’s) behavior, and affect the outcome.
As such, there is a link between changing situation and governing variables, a link between changing situation and action strategies, and a link between changing situation and consequences. Figure 33 depicts these linkages over the Argyris and Schon’s single- and double-loop learning model.

**Figure 33: Incorporating Responsive Learning into Single- and Double-loop Learning**

These linkages showed more than just the influences between changing situation and governing variables, action strategies, and consequences. From a learning perspective, it is the sensitivity and responsiveness of the organization and people to the changes around them that enable them to consider or evaluate the governing variables, action strategies, and consequences against those changing situations.

This form of learning exhibits both single-loop learning and double-loop learning. It is single-loop learning when responding to changes, mostly at the micro, event level, during the execution of the action strategies, making real-time, or near real-time changes to those actions as desired based on the changes detected, and emerging risk incident identified. This cannot be double-loop as it would stall the execution and response. In a dialectic conducted with Tay (2003) on the fault diagnostic expert systems that has been successfully implemented, it was learned that the operators of the machine needed to be responsive to emerging faults when the vehicle was in operation, and single-loop learning was therefore necessary for efficiency.

On the other hand, when designing the action strategies, and revising them for improvement following an actual incident or scenario-based testing, where the governing variables need to be carefully evaluated, double-loop learning based on macro-level changes identified within and external to the systems, including individuals, groups, and organizational systems behavior, threat and technology trends, and business directions are necessary to ensure that the governing variables are challenged and up-to-date.
Improvements in the action strategies in both design and execution would lead to improvement in readiness, and, as evidenced in this study, improvement of responsiveness of the organization to changes within and external to it. This also increases its sensitivity to ongoing changes in the risk environment. The essence of this form of learning may therefore be named as “responsive learning”, leveraging the single- and double-loop learning with a focus on the changing situations, both at the micro and macro levels.

The emergence of responsive learning within the responsive strategy provides for an integrated performance evaluation process within the approach. Through the learning processes (single- and double-loop learning), the performance of information risk manager (IRM) and the organization as a whole becomes clear.

While the actual performance cannot be pre-determined until an actual incident occurred, responsive learning enables the performance of IRM and the organization to be determined through the scenarios testing and drills designed as part of the responsive model (Figure 30). A poorly designed plan, or action strategy, or badly executed actions will likely result in undesirable outcome in response to the scenario tests conducted. A poorly devised scenario (with poor understanding of the risk environment) will also likely result in negative feedback from the participants in terms of their personal performance satisfaction in supporting the execution of the plan, as observed and experienced in Tay & Lim (2004; 2007). In an actual incident, as evidenced in this study (contrasting the outcomes interpreted and discussed in Sections 4.3.3 and 4.4.2), with poor preparation, the impact would also likely to be more significant. On the other hand, with proper planning and execution of action strategies of the responsive security model (such as the model devised in Figure 30), outcome of the scenario testing and drills would likely to be more positive. The performance measurements taken in such an approach, using scenarios testing and drills and responsive learning, therefore translates into higher readiness and responsiveness.

This means that the performance of IRM in such an approach have an impact on the outcome of incidents to the organization, rather than the count of incidents and control compliance gaps. The responsive learning process, used in conjunction with the responsive model (Figure 30) within the responsive strategy therefore addresses the performance measure issues raised in research question 3.
4.5 Discussion

The four major action research cycles, and their respective and iterative outcome analysis and interpretation have resulted in the development and validation of a social-technical approach, and a responsive approach to information security risk management, including the supporting framework and tools, in response to the three research questions described in Chapter 1. The research questions were confirmed as significant research issues in the current knowledge domain, as reflected in the gaps identified in the literature review presented in Chapter 2. The nature of these research questions encouraged the use of social science methods of inquiry, in which action research was found to be suitable and therefore adopted for the conduct of the study, as described in Chapter 3.

A fundamental problem in the information risk management knowledge domain is the circularity problem of the commonly used information security principles, as identified in Section 2.3. The circularity problem highlights a common discrepancy in the current principles, in which “weak links” prevail in the final outcome of their application, resulting in uncertainties in the information risk environment.

A primary outcome of this study is the discovery of the piezoelectric behavioral metaphor, which resulted in the development of a substantive theory, named as the piezoelectric theory of information risk management. The piezoelectric theory recognizes the existence of uncertainties and that complete identification and elimination of weak links is not a practical objective for information risk management. Based on the findings of this study, the theory is that an organization’s responsiveness to the anticipated and unexpected behavior of adversaries and organizational change events relates inversely to the potential impact of those actions of the adversaries or events on the organization. As such, in addition to the current approach of adopting a baseline standard (such as the ISO/IEC 17799 standards) and related principles and controls to manage information risk, organization should strategize information risk management with an increase focus on change events, situation awareness, and criticality alignment. Change events include planned changes, and unplanned, or unexpected changes, commonly resulting in “focusing events” (Birkland, 1997). Such an approach delivers the necessary piezoelectric behavior to improve the organization’s readiness to respond systemically to the actions of the adversaries, and other planned and unexpected changes in the risk environment.
An organization that is not responsive to the adversaries’ behavior and actions, and change events will experience more of an impact, which is likely to be significantly more severe, than one that is ready and responsive (i.e., the contrast in the outcomes in Sections 4.3.3 and 4.4.2 on the same set of security incidents that occurred in the period of the study). In the best case scenario (for the defending organization), the responsiveness of an organization will deter the adversaries’ action strategies, including insider threats. Otherwise, being responsive puts the organization in an alert position to actively respond to the adversaries’ actions in a timely manner, expending the adversaries’ resources and minimizing the impact on the organization (as in the use of the Sinkhole network against the Antinny Worm attack (J20061126) discussed in Section 4.4.8. This readiness position is better than one in which the organization is unable to act even with knowledge of the changing risk situation. When readiness is not a focus item in the organization’s information risk management strategy, valuable resources will continue to be expended to address only the known risks to achieve a state of compliance with either the internal or regulatory policies, or both, and management will constantly be surprised by the attackers breaching the security of its information systems (as discussed in Section 4.2 and 4.3).

**Figure 34: Resolving the circularity problem of information security principles with the introduction of piezoelectric behavior principle**

The principle of the piezoelectric behavior in such an approach, supported by the findings of this study, therefore provides a possible resolution to the circularity problem, as depicted in Figure 34, supporting and extending the existing principles to improve the organization risk readiness status, but not resulting in the same issues that those principles were set out to resolve.

As learned from the literature review discussed in Chapter 2, and the issues and dilemmas discussed in Section 4.2, in addition to being responsive to changing events, the information risk management strategy needs to place focus on the organizational stakeholders’ interest and influence their commitments. The study through action
research cycles 2 and 3 established that a social-technical approach leveraging existing social science inquiry techniques, and systems thinking tool is suitable for gaining the required understanding of stakeholders’ concerns and agenda, resulting in the development of integrated tools such as the Five-level Action Map (FLAM), and the SECD4 risk management process, and implementation of action learning sessions as part of the IRM Program. Using the concept of criticality alignment, which is part of the piezoelectric theory developed in the final action research cycle of the study, further improved upon the stakeholders’ engagement tactics. Criticality alignment exhibits a concept similar to the idea of establishing a focal point in the “Bargaining Theory” in Schelling (1960, pp. 21-52), and Dick’s (1997b) dialectic analysis technique of analyzing disagreements to establish agreement, as described in Section 3.3.3.2.1. Using criticality alignment, a common focal point can be established between the risk manager and business management, which helped to improve understanding on disagreements, and bring agreements on risk issues critical for the business to address. This approach addresses a common shortcoming in the traditional risk management approach that was applied in the organizations studied, in which the concerns over business resources, and uncertainties over significance of risk issues often resulted in a trade-off between business and risk management, a win-lose situation that does not address the underlying risk issues when the business opportunity “wins”. In reality, it is the adversaries who will stand a better position to “win” from such a trade-off.

The responsive approach, and the social-technical approach, both validated in their conceptual construct and ecological validity through the action research cycles, also exhibited a form of responsive learning (see Section 4.4.10), incorporating both single-loop, and double-loop learning behaviors, catering for the needs of different situations, based on the organization’s situation awareness, depending on the changing events involved.

These principles, concepts, and tools, developed through this study provide clear contributions of knowledge to the information risk management domain and answer the three research questions involved in this study, as discussed below.

Research question 1: What should an Information Risk Manager do differently or change in his/her strategy and plan, in managing information security risk for the
organization in order not to result in a compliance driven and/or control-oriented security culture?

This study revealed that traditional approach of information risk management as practiced in the organizations studied, which relied primarily on baseline standards, subjective output of risk assessment methodologies, and the use of controls to resolve identifiable information risk issues is often problematic, and does not provide the outcomes desired. As validated in this study, based on the piezoelectric theory of information risk management, Information Risk Manager should adopt a responsive approach in developing the organization’s information risk management strategy and plan. The responsive approach directs the organization management focus on the readiness of the organization systems to respond to change events, including unexpected security events, and planned changes in the risk environment, by improving its situation awareness, and identifying and implementing criticality alignment. To be ready, an organization needs to undertake action strategies and activities, including scenarios planning, testing, and drills, that prepare individuals and systems to respond to unexpected change events that could be unidentifiable initially, residual in systems implementation, error in risk assessment, or due to the causality of other events, in addition to be in compliant with the policies of addressing known risks based on risk assessment. The responsive approach does not replace or deprecate the needs for existing supporting tools and methodologies, as they are necessary for meeting regulatory and policies requirements, and addressing known risk issues that would otherwise allow the adversaries to achieve their objectives more easily. Closures of known risk issues, through traditional approaches, will provide more resources and focus to readiness for unexpected events and related risk issues. This brings about a renewed meaning to traditional risk management approaches, which is about addressing known risk issues instead of simply about policy and regulatory compliance.

Research question 2: How should Information Risk Managers manage the information security risk in a constantly changing business and IT risk environment, such as (1) security risk development in the information technology arena that could disrupt the business and/or IT operations, and (2) changes in the business and/or IT strategy and implementation that could significantly change the organization’s risk posture?
The significance of change events severely affecting the organization’s business continuity and IT services availability was experienced in several instances in the early research cycles. The relevance of this research question in practice is therefore reaffirmed as part of this study. The responsive approach was developed as a result of these findings as well, since there are uncertainties that cannot be identified and controlled in the traditional approaches, and being ready to respond to any eventual occurrence is therefore a logical approach to address change.

Change events, which include (1) unexpected security events and resulting focusing events, and (2) planned changes, as highlighted in the research question, are identified as a key element of the piezoelectric behavior. The responsive approach, which is developed based on the substantive piezoelectric theory, involves developing and implementing strategy and plans that identify and detect change events, improve organization’s awareness of the changing situations, and prepare the organization to be able to respond systemically based on the needs for criticality alignment. As discussed in Section 4.4.6 and earlier in this section, criticality alignment, one of the three key elements of the piezoelectric behavior, brings business management and information risk managers to a common focal point to ensure systems and resources most critical to the organization are aligned to ensure adequate protection and prepared to respond to those change events anticipated and unexpected.

To manage information risk in a constantly changing business and IT environment, as supported by the findings of this study, Information Risk Managers should implement a responsive approach. To do this, Information Risk Managers need to establish a clear understanding of the business risk environment, including the social-technical aspects. This can be achieved through the use of the IRM framework (Appendix D) developed and the Dialectic Model adopted and verified in this study (Section 4.3). With this knowledge and understanding of the business risk environment, Information Risk Managers will then be able to develop suitable strategy and plans to provide an IRM system with specific programs and projects to achieve the information risk management objectives in line with stakeholders’ agenda. The study developed the FLAM (Figure 21) and the SECD4 social-technical process (Figure 22) and validated their applicability in the practice environment. The action strategies and related IRM Programs in the IRM system needs to be updated constantly based on data gathered from the changing risk environment, including emerging events and output from the
actions of the adversaries. The IRM Systems Model (Figure 30), which evolved from the outcome of the study and analysis of related results, provides an initial model for establishing a continuous flow of risk information for analysis and updating of the action strategies in response to changing events affecting the organization. In addition, IRM needs to provide the necessary education and training to improve situation awareness and competency of information risk managers and organization staff based on individual and group roles and responsibilities, in relation to the potential risk scenarios and known patterns of risk events experienced from the organization’s learning experiences. Scenario-based training and drills are found to provide the required outcome for adoption to fulfill the need for situation awareness.

Research question 3: How should organizations resolve the conflict between the performance measurements of the Information Risk Manager and the outcome of a security incident? Should the Information Risk Manager’s performance reflect the security risk status of the organization, or, in other words, what should the relationship be between her/his performance and the security status of the organization?

As discussed in Section 4.2.8, a systemic analysis of the causality of information security revealed that when the risk situation improved (as a result of less damages or losses), the tendency is for the organization to reduce its resource investment in activities that would help to improve security in the system environment, including people, processes, and technologies. Similarly, when information risk managers’ strategies and actions have helped to improve the risk status, resulting in less or no incident, or when security events are well managed such that they did not result in negative impact, the outcome is unaccountable\textsuperscript{124}. The lack of “outcome” could not be used to demonstrate the efficacy of the information risk managers directly, since it did not exist in the first place. Business management will also be skeptical of the needs for information risk managers to continue their level of spending on security. On the other hand, when the organization’s information risks are not adequately managed, breaches are likely to occur. As this study has shown, organization in such a situation will suffer from losses or damages from both expectable and unexpected security events. The performance of information risk managers will be questionable. The use
of risk status to measure the performance of information risk managers will therefore be paradoxical.

As also tested in this research study through the use of a social-technical approach, supported by the use of a RAG scorecard system (Section 4.3.1.6), a control- and compliance-based scorecard could not provide an effective and meaningful measure of the risk status of the organization, and using such a system to measure the performance of information risk managers is therefore unfair to the risk managers.

Instead of measuring the risk status, or compliance status, to determine information risk managers’ performance, the study concluded that a responsive approach, incorporating measurement through the use of scenarios testing and drills, provides a more effective, meaningful, and fair measure of performance of the risk managers, as well as the security readiness of the organization. As stated in the piezoelectric theory, based on the findings of this study, an organization’s responsiveness is indirectly proportional to the significance of impact that the organization will incur in face with a security event, or a focusing event. The capability of the organization’s people, processes, and technologies to respond and align with the changing risk situation, which demonstrate the organization’s responsiveness, therefore presents a systemic metric for measuring the security readiness of the organization, the performance of the risk managers, as well as related stakeholders in the organization. Such metrics can be taken during the conduct and evaluation of the scenarios planning, testing, and drills processes, designed for improving the readiness of the organization. An organization that is not ready is therefore less responsive, and, as shown in this study, will incur a higher impact. An organization’s readiness to respond, which can be tested using scenarios-based tactics, can be improved by IRM strategy, plan, program, and actions, with stakeholders’ participation. The reverse is also true. As such, there is a direct relationship between organization’s readiness to IRM and also to stakeholders’ actions. Measuring readiness (and hence, responsiveness) is therefore meaningful and fair to the stakeholders (including information risk managers) involved.

In this study, a qualitative approach was undertaken to determine the readiness of the organizations to respond to unexpected security events. This includes assessing the comprehensiveness of the program and activities undertaken for readiness, and the outcome in terms of stakeholders’ participations and feedback. This approach showed
what has been done, but not necessarily how ready the organization is, and did not provide the required level of situation awareness on a continuous basis.

As discussed in Section 4.4.9, the concept of a responsive index has also been suggested. Such an index (as a quantitative indicator), if used, should be assessed against the risk forecast, which should encompass risk indicators from public information sources, and threat trends that are relevant to the organization. It should assess the readiness status of individuals, groups, as well as IT infrastructure and systems with regard to their understanding and knowledge of what should be their roles and actions for the range of security scenarios that are envisaged from the developing threat trends and risk forecast.

Given that there are different methods of quantitative measurements currently being researched and standardized, and a practical metric warrant a separate study to ensure its efficacy, fairness, and meaningfulness, from the Four-window system perspective, I propose this to be a topic for future research studies.125

The lack of a responsive index is not however a significant issue in the responsive strategy. From the perspective of “Responsive Learning” as analyzed and discussed in Section 4.4.10, in which an action research-based cyclical process is implemented as part of the responsive strategy, the action strategies derived and executed, which affect the readiness of the organization, are evaluated against the organization’s information risk management plan and outcome (in actual incidents as well as scenario testing and drills). This process, incorporating single- and double-loop learning, is itself about performance evaluation, even without a quantitative responsive index. This in fact has the advantage of avoiding the negative effects of a quantitative performance indicator (i.e., the responsive index), in which individuals develop an inclination to focus on a quantitative measure (like focusing on the color in the case of a RAG Scorecard) instead of the underlying issues involved when the outcome and the plan are mismatched. From a learning perspective, the integrated responsive learning within the responsive strategy provides more value for improving the subsequent plan and action strategies. The responsive learning process provides direct accountability for the IRM’s plans and activities for the responsiveness and readiness action strategies, eliminating the dilemmas of incident counting and compliance measurement as experienced in the earlier action research cycles as
discussed in Section 4.3.1.6. This addresses the problems underlying research question 3.

In summary, this study has identified a suitable metaphor for assessing and improving organizational behavior relating to information risk, resulting in the development of a new substantive theory for information risk management. This study has also developed and established a set of tools and tactics that collectively provide for implementing a responsive strategy of managing information security risk, based on the piezoelectric theory. As reported in action research cycle 4 (J20061126), and discussed in Section 4.4, the responsive strategy has been validated within the context of this study to be effective for gaining stakeholders’ buy-in, as well as practical for implementation in the practice environment, as a response to the different, and more importantly, changing risk situations, resulting from the actions or behavior of adversaries.

The piezoelectric theory remains a substantive theory at this point, as its implementation is limited to the scope and coverage of this study, within the resources available. Nevertheless, it provides a basis for gaining a new perspective and understanding of information security risk management in organizations, at least to those similar to this research, therefore contributing to the knowledge domain. With evolving understanding through the use of the responsive strategy by more organizations and individuals going forward, we can envisage new tools and tactics will also be developed to support improved implementation of the strategy in the near future.

4.6 Chapter Summary and Remarks

This chapter has described the key findings and understandings, and outcomes involved in the action research cycles, including data analysis and interpretations conducted through the research study from January 2002 to December 2006.

We begin with the findings that improved our understanding of the issues and dilemmas in information risk management in the practice environment, which established the key issues to be addressed and set the path for the progress of the study. The understanding led to the development and implementation of a social-technical approach, and a responsive approach, to address those issues and dilemmas.
involved, which are captured in the three research questions. The testing and evaluation conducted through the social-technical approach confirmed that such an approach is suitable for addressing the “soft” aspects of information risk management, in particular, for understanding stakeholders’ agenda, and gaining their commitments and supports in the IRM program and activities. The testing further disconfirmed the validity of tactics such as the RAG Scorecard for measuring risk status, and that compliance and controls are adequate approach for managing information risk.

The validity of the social-technical approach is supported by the direct application of the concepts, tools, and tactics, in the practice in organization ALPHA.

The validity of the responsive approach is supported by case studies of actual practices in organization BETA, two significant security incidents, and one focusing event (Tsunami disaster), all of which occurred during the course of the study. These case studies support the construct validity of the responsive approach. The responsive approach was also implemented in organization CHARLIE, and used as a strategy for stakeholders’ alignment, resulting in significantly positive outcome in the standardization arena in Singapore. The practical applications support the required ecological validity for the responsive approach. The validity of the piezoelectric theory as demonstrated by the validity of responsive approach, supported by the outcomes of this study, is further supported by the lack of disconfirming evidence through discourses conducted with more than 30 other fellow practitioners in other organizations, in a variety of settings, including questionnaire based survey, interviewing, dialectics, and numerous roundtable discussion in security conferences, adding more rigor to the development of the concept, and related tools and tactics as the approach evolved through the course of the study.
5 Conclusion and Implications

“Answers are merely places to rest for a moment. They are not final.”

Richard Paul and Linda Elder
The Art of Socratic Questioning

5.1 Introduction

This research study began on an exploratory basis on the issues, dilemmas, and approaches associated with the existing practice of managing information risk in organizations. The literature review in Chapter 2 identified a problem of circularity in existing principles that have been widely adopted for attaining information security, and that current knowledge have been focused predominantly on the protection of information and information systems, and are biased toward the engineering and use of mitigating controls for addressing information risk issues. There was also a lack of knowledge and studies in existing literature on managing information risk in a changing risk environment, which has also been a problematic issue in the practice domain. The purpose of this study was therefore to understand the issues and dilemma face by professional risk managers in the practice environment, and to develop an approach for managing information risk in enterprise organizations, suitable for addressing those issues and dilemmas involved in the changing risk environment. This resulted in the formulation of the three primary research questions for the study.

Chapter 2 further identified the needs for, and the lack of, social-technical studies in this problem domain, which Chapter 3 identified, described, and justified action research as the meta-methodology suitable for the conduct of the study, and also the primary methodology for data collection. The research procedures and the chronology of events in the Action Research Cycles are also described in Chapter 3. The analysis and interpretation of data collected through the action research cycles, presented in Chapter 4, led to the derivation of the piezoelectric theory for information risk management, supported by a responsive strategy for achieving the purpose of this study. It addresses the research questions, which are the major contributions of knowledge in this study.
Chapter 5 – Conclusion and Implications

This final chapter begins with a recap of the research questions to determine if the purpose of the study has been met, and draws attention to the major contributions of this thesis.

This chapter also follows Perry’s (1998) suggestions by including discussions of the implications of the developed theory, strategy, and approach for existing theory, organizational policies, and practitioners of information risk management. The discussions are followed by deliberations on possible directions for future research arising from the findings of this study, and the limitations of the piezoelectric theory for information risk management. The chapter is concluded with a personal reflection on the research experience.

5.2 Conclusions about Each Research Question

Beginning in Chapter 1, the primary questions that guided this study were:

1. What should an Information Risk Manager (IRM) do differently or change in his/her strategy and plan when managing information risk for the organization in order not to have a compliance driven and/or control-oriented security culture as a result?

2. How should IRMs manage the information risk in a constantly changing business and IT risk environment, such as (1) security risk development in the information technology arena that could disrupt the business and/or IT operations, and (2) changes in the business and/or IT strategy and implementation that could significantly change the organization’s risk posture?

3. How should organizations resolve the conflict between the performance measurements of the IRM and the outcome of a security incident? Should the IRM’s performance reflect the security risk status of the organization, or, in other words, what should the relationship be between her/his performance and the security status of the organization?

In Chapter 2, existing literature relating to the principles, practices, approaches, and key recurring research concerns and studies were reviewed. While there are increasing calls for a change of paradigm, including more emphasis on a non-technical approach, such as social, economic, and social-technical studies of the problem domain, there remains a lack of studies on managing change and inadequacies in performance
measurement for information risk management. Existing literature emphasizes a number of security principles, such as *weakest link, defense in depth, no perfect security,* and *risk management,* which was found to create a problem of circularity for risk managers, and to promote a control-oriented and protection biased approach to information risk management. The literature review therefore confirmed the relevance and importance of the research questions. This research study has started addressing such voids in the literature, and expands academic and practitioners’ understanding of information risk management in general.

The main issues in Research Question 1 relate to the focus on regulatory and policy compliance, and the consequential practice of implementing mitigating controls as the primary approach to achieving the objectives of information security. Regulations and policies, however, are often focused on known risk issues, in particular, those that have already caused significant disruptions to businesses, but pay little attention to risks that are unknown or not made known to the regulators and policy makers. Implementing controls for compliance purpose and achieving compliance as such leaves potential security gaps for exploitation. The literature review in Chapter 2 established the prominence of compliance-driven security implementation, which was also found to be an increasing trend in recent years.

In the practice environment, the study, however, established that compliance addresses regulatory risks, but does not necessarily achieve information security needed for the organization. As experienced in this study, IRM expended most of its resources in achieving compliance by undertaking activities that helped to deliver a more positive audit result rather than reviewing security events, and addressing specific risk issues. In addition, the organization in which this study was conducted, and information risk managers were caught off-guard, and disruptions to IT and business operations resulted when new security vulnerabilities were discovered, when new worm programs attacked the corporate network, and when the SARS epidemic required unprecedented changes to IT infrastructure for business continuity. In these incidents, the organization’s business continuity and disaster recovery plans, which focused on scaled-down operation and recovery, could not be activated or leveraged to respond systemically to minimize the disruptions. Security controls implemented for compliance reasons became obstacles when the business and IT departments were responding to those situations, resulting in calls to bypass policies and the disabling of
security settings, heightening the information risk to the organization when the situation required the provision of better security.

The analysis and interpretation discussed in Chapter 4 on the data collected from the Action Research Cycles concluded that instead of focusing on compliance to achieve information security objectives, information risk managers should focus on preparing the organization to be ready to respond systemically to the changing risk environment.

This conclusion was drawn from the development of the substantive theory, known here as the piezoelectric theory for information risk management. Piezoelectric is a kind of electromagnetic material that is highly responsive to external pressure, such as a squeeze on its surfaces, which triggers an immediate alignment of all its electrical charges in a single direction. The theory is that an organization’s responsiveness (to have its resources aligned) to the anticipated and unexpected behavior (i.e., the triggers) of adversaries or the occurrence of information risk events relates inversely to the potential impact of those actions of adversaries or events for the organization.

As found in this study, an organization that is not responsive to adversaries’ behavior and actions, or related information risk events will likely experience a more severe impact than one that is more responsive. In the best case scenario analyzed (for the defending organization), the responsiveness of an organization will likely deter adversaries’ action strategies. Otherwise, responsiveness puts the organization in a position that is ready to respond to adversaries’ actions in a timely manner, expending adversaries’ resources and minimizing, if not eliminating, the impact on the organization. This position is better than one in which the organization was unable to act even with knowledge of the changing risk situation and continues to focus on expending valuable resources to address only the known risks to achieve a state of compliance with either the internal or regulatory policies, or both, while constantly being surprised by attackers breaching the security of its information systems.

The piezoelectric theory suggests that IRMs should develop and implement a responsive strategy for managing information risks. The responsive strategy is concerned with change events, situation awareness, and criticality alignment. These three elements assimilate the squeeze-trigger-alignment sequence, as in the piezoelectric material. Change events relate to the organization’s knowledge of the adversaries’ actions, including anticipated and unanticipated actions, actual probes, and attacks as they unfold and emerge, the related events, and the associated
weaknesses in the organization. Situation awareness relates to the organization’s sensitivity to changing risk situations. Criticality alignment means ability and readiness of the organization to respond in the most appropriate manner, focusing on critical system elements, addressing known risk issues promptly and systematically, and preparing for the unknowns, causing adversaries to fail in their attempts to attack the organization. Failure is incurred by adversaries when their actions are ineffective (when the weakness is known and has been addressed), discovered and responded to promptly (when the weakness was unknown before the attack), and leaving them with little or no gain from attacking the victim organization.

The responsive strategy determines and derives actions from change events. Change is therefore the main focus for improving responsiveness. This addresses the main concern raised in Research Question 2, which involves both planned and unplanned changes that affect the organization. In terms of planned change, the related change events and associated risk can be pre-determined and managed through collaborative planning and execution between IRM and the stakeholders. Awareness in terms of the situations and changes involved, and corresponding alignment responses (including implementation of required security controls), can be programmatically communicated and executed. When a change is unplanned or unanticipated, continuous monitoring and event analysis provide for situation awareness, and exercises and training, such as scenario development, planning, walkthroughs and drills, prepare the organization to be ready, and will therefore be able to align responsively.

In terms of IRM’s performance and the organization’s security status in the practice environment, this study, as reported in Chapter 4, observed that the management of the organizations studied did not explicitly require the performance of IRM to reflect the security status of the organization, but, when security breaches occurred, IRM was often accountable. Given the cost involved in implementing and operating security controls, management is, however, concerned about the effectiveness of security. The need for compliance with regulatory and corporate policies also drives management’s demand for awareness of the security posture or status of the organization. Management expects that there will ideally be no security breaches or incidents, while having a few incidents is normally acceptable. “Few” is nevertheless a subjective measure, depending on how the IRMs justify the mishap in each incident encountered.
Nevertheless, having a poor audit rating and compliance issues were regarded as performance failure on the part of the IRM.

Performance measurement of IRM and the security status of the organization that they serve was therefore an issue in practice, but as established in the literature review in Chapter 2, there was no suitable solution offered in existing literature. The gap in the literature highlighted a need and an opportunity for knowledge contribution. Addressing Research Question 3 was therefore important, given management’s vested interest in this area to ensure that the cost incurred in information risk management was allocated effectively and efficiently, and the need for the value of IRM to be recognized and realized.

The Action Research Cycles conducted in organization ALPHA, as described in Chapter 3 and analyzed and interpreted in Chapter 4, attempted the use of a Scorecard approach for measuring IRM’s performance and the organization’s security status. This produced a negative case that disconfirmed the effectiveness of such an approach, contributing to further understanding on the issues and dilemmas in performance measurement and security status.

The responsive strategy directs the attention and activities of IRM towards responsiveness and hence security readiness. According to the piezoelectric theory, as supported by the findings of this study, an organization’s responsiveness relates inversely to the potential impact that it will experience when a security weakness is exploited. This means that the security posture or status of the organization is weak if the organization is not responsive. Responsiveness therefore reflects the performance of IRM. This approach differs from a compliance-based performance measurement in that it caters to both known and unknown risk and changes. A fully compliant organization and a highly responsive organization will both have security weaknesses. The difference is that the latter will be able to respond and more likely able to manage an attack exploiting those (known and unknown) weaknesses, and as such, likely to suffer a less severe impact than the former. Within the limitation and scope of this study, this assertion was found to be true comparing the outcomes of related security incidents between organization ALPHA and BETA. Furthermore, responsiveness can be tested programmatically or systematically, but not the state of security, when unknown risks are considered. Besides being effective, reliable, and efficient, the focus on improving responsiveness, which has a direct relationship with the outcome
of a security event, becomes meaningful to the IRM. IRM’s knowledge and experiences on change events, situation awareness, and critical alignment influence such outcomes in the organization. Assessing IRM’s performance based on responsiveness of the organization is therefore fair, and does not require the occurrence of an actual security incident for confirmation. Similarly, the efforts and activities of stakeholders, including end-users of information systems, contribute to the responsiveness of the organization as a whole. Assessing performance based on responsiveness is also a fair approach compared with a security policy compliance approach. From a systemic thinking perspective, the responsive strategy satisfies the criteria identified in Flood’s Four-windows systemic view, which includes (1) effectiveness and reliability, (2) efficiency, (3) meaningfulness, and (4) knowledge power (fairness). The piezoelectric theory therefore provides a systemic approach for resolving the problems identified in Research Question 3.

In summary, the piezoelectric theory accomplishes the purpose of this study. The study contributes to the understanding of the issues and dilemmas faced by professional information risk managers in the practice environment, and the piezoelectric theory provides an approach – the responsive approach – for addressing those issues and dilemmas involved in the changing risk environment. The study further identified, developed, and validated a set of tools and developed a systems model suitable for implementing the responsive approach to enhance the success of the responsive strategy.

In the next section, the significance of the research problem and major contributions of this thesis are highlighted.

5.3 Conclusions about the Research Problem

This study has contributed to the understanding of the issues and dilemmas in managing information risks in organizations spanning across Australia, China, Indonesia, Japan, Malaysia, The Philippines, Singapore, South Korea, and Thailand, and this may be of significance to the financial industry and other multi-national companies in general. The major contribution of this thesis is the piezoelectric theory to the knowledge domain of information risk management, by offering a new perspective and approach to manage information risk that will leverage the changing risk environment as a catalyst for organization alignment in terms of people, process,
and technology, to meet the objectives of information security of the organization.
The contribution to the theory occurs as follows.

The first contribution to knowledge is the development of the piezoelectric theory for
information risk management. The significance of this theory is in the contribution it
makes to information risk management literature by providing a new meaning—
responsiveness—to the objective of managing information risk in organizations, i.e.,
to improve the responsiveness of the organization in a changing risk environment.

Another significance of the piezoelectric theory is its resolution of the circularity
problem (described in Chapter 2) relating to existing security principles. The
piezoelectric theory recognizes the existence of weak links and the imperfection of
technology, process, and people in organizations, and enables them to be managed
systemically through its focus on change events, provision for situation awareness and
preparing the organization to be ready for critical alignment.

The second contribution from the development of the piezoelectric theory is the
elaboration of the responsive strategy. The significance of this contribution is the
understanding of the responsive approach gained through case studies and validation
testing conducted in the practice environment, supplemented by open dialogues with
fellow practitioners and analysis of a number of catastrophic natural disasters and
Internet security incidents that emerged during the period of the study. The
understanding led to the formalization of the concepts and processes required for
establishing the piezoelectric behavior, encompassing change events, situation
awareness, and critical alignment to achieve responsiveness in information risk
management. The description of the understanding and knowledge gained in Chapter
4 provides the base knowledge for IRM when testing, implementing, or conducting
further research of the responsive strategy in another organization setting.

Another significance of this contribution is the development of a responsive system
reference model, i.e., the IRM Systems Model (Figure 30), that evolved from the
learning and understanding achieved through the case studies and test implementation
described in Chapter 4. The reference model incorporates a set of governing variables,
including regulatory policies, customer expectations, trends in technology and
security developments, and the established IT and business systems in use in the
organization to form the basis of the information risk management system. The
concept of piezoelectric behavior is integrated through additional components for identifying and capturing change events, and improving situation awareness and action strategies that provide for the needs for critical alignment of the organization in the changing risk environment. The reference model provides a basis for the responsive approach to be further developed and implemented by the IRM in other organization environments, and research for future studies of the responsive strategy and implementation.

The third contribution of this study is the successful adaptation of existing methods and tools such as the Singapore Standards, SS493 – *IT Security Standards Framework* (SPRING Singapore, 2001), and the Dialectic Model of Systems Inquiry (DMSI) described in Dick (2002f) and Tay & Lim (2004; 2007) for determining the governing variables, implementing and testing the validity of the responsive approach, and adopting the notion of critical alignment in the practice environment. This contributes to the extension of existing tools and techniques in both the information security and social studies knowledge domains, respectively, and demonstrated the applicability of action research techniques, such as the Dialectic Model, for developing action strategies for implementation in the information risk management problem domain.

The fourth contribution is the new understanding and knowledge of the issues and dilemmas with respect to the social aspects, such as managing stakeholders’ expectation and perceptions that facilitate the implementation of an information risk management program. The outcomes and contributions extend our knowledge of existing approaches by providing rich details and insights into the dynamics of the social processes that influence the work of the IRM, and his/her relationship with the stakeholders, related also to the issues of trust, controls, influence, and decision-making in managing information risk (Section 4.2). These understandings also led to the derivation of the Five-level Action Map (FLAM) (Figure 21) and SECD4 social-technical process for operating an information risk management system (Figure 22) based on analysis and interpretation of the initial Action Research Cycles conducted as part of this study. The FLAM identifies and describes the hierarchy of plans, programs, projects, action strategies and events, and the relationship of these components in an information risk management system. The SECD4 social-technical process for operating an information security management system, based on Argyris & Schon’s (1991b) *Double-loop Learning*, integrates social studies techniques such as
stakeholder analysis, entry and contracting, convergent interviewing, dialectic data analysis, and Robert Flood’s (1999) Four-windows systemic view, into the risk management process, which supported the possibility and benefits of a social-technical integrated approach as proposed in propositions 2 to 5 (in Section 2.8) synthesized from the literature review in Chapter 2. The FLAM, SECD4, and DSMI social-technical processes provide another set of tools that can be used readily by both novices and experienced IRMs in the execution of their roles, and, at the same time, a basis for researchers to conduct further research in this area.

Finally, the application of action research as a meta-methodology and research methodology, including Dick’s (2000b) data-driven analysis technique, Flood’s (1999) Four-windows systemic view, and Argyris & Schon’s (1991b) Theory of Action for data analysis and interpretation in the field of information risk management are a contribution to knowledge. The piezoelectric theory that emerged from the action research process adds significantly to the knowledge domain, by being the first action research study of information risk management in the Asia Pacific region. Applying the piezoelectric theory in the case study analysis and using it in another organization indicated that responsiveness is increasingly being recognized as an important focal point for risk management, and the use of the responsive strategy, focusing on change events, situation awareness, and critical alignment, improves stakeholders’ commitment much earlier in the process. This enables IRM to focus on the objectives of information risk management, and the organization to be prepared for both known and unknown risks in the changing IT and business environments.

The successful development of the responsive strategy and supporting tools and tactics based on the piezoelectric theory is a contribution to the methodological literature.

5.4 Implications for Theory

The piezoelectric theory and the responsive strategy suggest five implications for theory, and five implications for policies and practices in the field of information risk management, as well as other related and relevant fields and industries.

The first implication for theory relates to the objectives of information security. The development and successful application of the piezoelectric theory in this study confirmed the first proposition synthesized the literature review in Section 2.8. The
outcome of this study suggests responsiveness to be one of the objectives of information security—i.e., to improve the responsiveness of the organization to a changing risk environment—in addition to the five common objectives that were synthesized from the existing literature reviewed in Section 2.2. This extension is supported by the piezoelectric theory, which will focus researchers’ and practitioners’ attention on the piezoelectric behavior as a metaphor for information security, and the approach of focusing on change events, situation awareness and critical alignment, to facilitate progress beyond the current methods of achieving information security.

The second implication for theory relates to responsiveness as an information security principle. As highlighted in the earlier sections, the piezoelectric theory resolves the problem of circularity inherent in existing security principles when they are evaluated as parts of a system. Responsiveness introduces a new perspective to the theoretical discourse on the principles of information security (in Section 2.3). As part of the strategy, responsiveness addresses both the “weakest link” and “no perfect security” related concerns, and is able to leverage risk management, use of technology, and defense in depth principles to improve an organization’s situation awareness and readiness for critical alignment.

The third implication for theory relates to the strategic thinking and approaches applicable to information risk management. The piezoelectric theory suggests responsive strategy as a strategy addition to the traditional Protect-Detect-React, and Detect-React-Protect strategies discussed in Section 2.4. The responsive strategy resolves the weaknesses of these former strategies (as elaborated in Sections 2.4.1 and 2.4.2), and addresses the requirements, which call for more strategic thinking in Section 2.4.3.

The fourth implication for theory relates to the IRM System Reference Model (Figure 32), which as discussed in Chapter 4, exhibits both Single- and Double-loop learning. Single-loop learning is used when responding to changes, mostly at the micro, event level, during the execution of the action strategies, making real-time or near real-time changes to those actions as required based on the changes detected, and emerging risk incident identified. This cannot be double-loop, as that would stall the execution and response. On the other hand, when designing the action strategies, and revising them for improvement following an actual incident or scenario-based testing, where the governing variables need to be carefully evaluated, double-loop learning based on
macro-level changes identified within and external to the systems, including individuals, groups, and organizational systems behavior, threat and technology trends, and business directions are necessary to ensure that the governing variables are challenged and up-to-date. Improvements in the action strategies in both design and execution would lead to improvement in readiness and responsiveness of the organization to changes within and external to it. This also increases its sensitivity to ongoing changes. This infers that a combination of both Single- and Double-loop learning in an organization’s information risk management system is important for responsiveness. We call this emergent property “Responsive Learning”, which suggests an emergent behavior of Argyris & Schon’s theory of Single- and Double-loop learning when applied as part of a responsive strategy in a changing risk environment.

The final implication for theory relates to the use of action research methodology in information risk management research studies. The outcome further affirms the applicability of action research as a methodology suitable for different disciplines, and a meta-methodology (Section 3.3.2.4) that enables the practice of methodological pluralism to achieve the desired outcomes. The outcome of this study adds to the collection of understanding and knowledge on action research, which provides another set of rich descriptions in the conduct of action research for other researchers and students interested in studying and expanding on the theoretical rigor of action research, and adopting it as a method of research in the context of their studies.

5.5 Implications for Policy and Practice

The rapid changes in the information risk landscape and regulators’ increased scrutiny for compliance purposes have increased the cost of information security, and instilled a compliance-focused and control-oriented information risk management system, which also means making things less flexible and adaptable to change. IRMs are expected to resolves these dilemmas, and to address the issues to enable business to function with agility to change, while remaining compliant with policies and regulations. The outcome of this study resolves these concerns with a responsive information security management system, based on the piezoelectric theory. In addition, as supported by the findings of this study, responsiveness provides a direct link to the security status of an organization, which enables the security readiness of the organization to be determined without the need for an actual security incident to
Chapter 5 – Conclusion and Implications

take place. The theory, and its supporting strategy and set of tools, therefore have important implications for policies and practices in the field. We discuss the five main implications below.

The first implication for policy relates to the opportunity for policy makers in both the public and private sectors to use responsiveness as a new motivation and yardstick for improving information risk management in organizations. This means establishing a policy to encourage the organization to provide an assurance of its information security status by demonstrating its capability and practice relating to change events, situation awareness, and critical alignment. Such a policy does not represent a depreciation of the existing practices of risk identification, assessment, and treatment, which address mainly known risk issues. In fact, it brings new meaning to such a process and related systems for managing known risk issues, which, when implemented, means removing change events relating to known risk issues that can be removed up front, therefore enabling the organization to focus on addressing new and emerging risks. In this regard, responsiveness provides a new motivation for addressing known risk issues, which means, improving the readiness of the organization to the changing risk environment. The ability of an organization to respond to a changing risk environment provides a direct assurance to regulators and policy and decision makers about the potential outcomes when an anticipated risk materializes, as well as when an unknown risk surfaces. This is better than having a conditional assurance that a risk is under control because the policies have been complied, but subject to the reliability of the risk assessment, and excluding issues that will potentially arise due to unanticipated human failures and risk compensation, which will result in unknown impact to the organization.

Second, as discussed in an IT auditors’ conference (Kang, 2005e), the changing information risk landscape, and the development of the piezoelectric theory also suggest new practices for the assurance professionals. Auditors and security assurance professionals should revise their scope of action in order to gain assurance about the responsiveness of an organization’s information risk management system. The existing methods of compliance testing about the integrity and reliability of controls remain important to assure that known risk issues are being addressed. A technique, known as scenario testing, which is analyzed and discussed in Chapter 4, which
enables the organization’s responsiveness to change events, situation awareness, and critical alignment to be determined, can be leveraged for responsiveness assurance.

Thirdly, the development of piezoelectric theory, which was fueled by observations made during the critical period of the SARS epidemic, when IT infrastructure systems were unable to respond to the changing risk situations even though the situations unfolded over a long period of time, suggests that new strategies and thinking on IT infrastructure planning and design are also necessary, and should have a focus on responsiveness. This may include an infrastructure provision, such as a Sinkhole network, for handling sudden attacks like the Antinny Worm incidents analyzed in Chapter 4, vulnerability management for responding to software update requirements, and flexible design and implementation that leverage the distributed nature of the Internet to improve responsiveness to security and catastrophic events—for example, by introducing policies and designing infrastructure incorporating security capability to support home computer systems and broadband Internet use, and encouraging frequent use of such capabilities that will improve situation awareness and critical alignment among the end-users so that an organization’s reliance on corporate computers and networks can be reduced over time. It is important to note that, while numerous technologies already exist to support such strategy requirements, their development was not motivated by the piezoelectric theory. There is therefore an opportunity for new innovations when technology developments are aligned to the responsive strategy.

The fourth implication relates to the structure and composition of information risk management and other related units in an organization. As analyzed in Chapter 4, existing Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), and Emergency Response (or Crisis Management), are focused on recovery of the business operations or IT infrastructure, in the aftermath of an incident. Each of these is called upon depending on the nature and timeliness of the incident. In practice, the processes and systems supporting these different units of organizations often overlap, which results in additional cost and duplication of efforts. The piezoelectric theory implies a gap in the existing system, between controls and recovery, which is using responsiveness to detect an emerging event (through situation awareness) to reduce damage, and to enable the business to continue to operate (through critical alignment), avoiding failure as much as possible. This, again, does not deprecate the importance
and relevance of BCP, DRP, and ER, since responsiveness does not eliminate failure, but suggests a possible evolution of these different functions to a new level that enables the organization to leverage the understanding and knowledge of continuity, recovery, and response, by organizing these functions as part of a readiness group focusing on responsiveness. The notion of critical alignment may also be extended to include recovery as one of the components that will bring the critical business functions back to align with the changed situation. This implication has been suggested in the 5th RAISS Forum meeting, and ISO/IEC JTC1 SC27 working group, which resulted in the initiation of a study in the ISO/IEC standards arena in late 2006.

The final implication relates to the practice of IRMs. For novice IRM and other information security practitioners who are new to the field of information risk management, the piezoelectric theory and the concepts of responsiveness and responsive strategy will be a useful starting point for learning and understanding how information risk may be managed in a changing risk environment. The piezoelectric theory will provide new practitioners with a balanced perspective and a strategy that enable them to address both known and emerging or unknown risks simultaneously. It will help the new practitioners in addressing the issues and dilemmas of previous approaches when faced with the changing risk situations in the business and IT environment. For experienced IRM and other information security practitioners, the piezoelectric theory and responsive strategy provide a fresh perspective and approach to the recurring issues and dilemmas of managing the changing risk environment. As the responsive strategy does not deprecate existing approaches, an experienced IRM will be able to leverage the learning and understanding of the piezoelectric theory to re-focus his/her management strategy and plan to have a focus on responsiveness over time. In both cases, the SS-493 adapted framework for information risk management governing variables (FIRM), Five-level Action Map (FLAM), SECD4 process, Dialectic Model for Systems Inquiry (DMSI), and IRM System Reference Model collectively provide the required tools, process, and model for learning and establishing a responsive information risk management system in an organization. In an organization in which an information risk management system is already in operation, the IRM, whether novice and experienced, can use the adapted framework to learn and understand the existing system, and the social-technical process for
stakeholders’ interactions, before suggesting suitable actions for improvement. The FLAM and IRM System Reference Model can similarly be used to determine if there are gaps in the existing system, and the action strategies required for implementing a responsive information risk management system. To enable the above undertakings for both new and experienced practitioners to understand and implement the responsive strategy, education and training will also be necessary. This should include training on the related methods of inquiry, such as action research and the dialectic modeling. The learning, understanding, and practice of these methods will further enable information risk practitioners to conduct their personal inquiries and improve their practices at the same time.

5.6 Suggestions for Further Research

The piezoelectric theory is a new development for information risk management, and this study has contributed valuable insights and assisted in understanding how it helps to resolve the issues and dilemmas of managing information risk in a changing risk environment. From it, several steps lie ahead for future research to advance the use, understanding, and formalization of the theory:

1. The piezoelectric theory, as described in earlier chapters, is applicable to the substantive area of inquiry, that is, the context of the financial industry and large multinational enterprises in the Asia Pacific region—Australia, China, Indonesia, Japan, Malaysia, The Philippines, Singapore, South Korea, and Thailand. Although it has been validated in a different organization locating in a different geography from where it was developed, the substantive nature of the theory cannot be generalized beyond the current area of inquiry. Substantive theories can, however, act as building blocks for a formal theory, which will then enable its application to a wider scope. One opportunity that was suggested in the earlier section that shows potential for such an elevation study is the expansion of the piezoelectric theory into other vertical disciplines that exhibit similar issues and dilemmas, for example, in business continuity, disaster recovery, and emergency response, or a higher—organization readiness—level covering all these areas. Conduct of research on the implementation of the responsive strategy in more organizations in different industries and geographic settings is another thread of development suitable for formalization of the theory. Although the elevation may extend the
usability of the theory, there are also caveats to watch for since every exploration will likely discover new categories, in particular, when the context and scope are broadened, which may give rise to new issues for practitioners and researchers. This, nevertheless, may also give rise to new discoveries or developments that provide further knowledge contribution and will enrich the field. Further research focusing on elevation of the theory is therefore worthwhile, and encouraged.

2. Along with the idea of generalization, there will also be benefits (from the knowledge enhancement and theory elevation perspectives) for further empirical research on the implementation and operation of the responsive strategy based on the piezoelectric theory to evaluate the consequences of such an approach over a longer period of time in an organization. This will then expose the strategy to more varieties of change events, and, consequently, enable further development of new techniques (or tactics) for improving situation awareness and critical alignment, and improve understanding of organization piezoelectric (responsive) behavior changes in relation to time and the change events (in terms of number, frequency, and other measures). With more exposure to change events, there may also be the possibility to further study and understand whether more specific patterns of relationships exist between responsiveness and the severity of impacts in relation to the tactics adopted or actions taken for determining change events, improving situation awareness, and increasing readiness for critical alignment.

3. Finally, while this study has resolved the issues and dilemmas of IRM performance versus security status of organization, we have not implemented a specific method for continuous measurement and reporting of the responsiveness status of an organization. This may be quantitative, qualitative, or a hybrid measurement scheme covering the organization’s understanding of the changing risk environment, and competence to execute of required actions for critical alignment. Further work to identify and develop the required tools, methods, and measurement suitable for presenting a responsiveness matrix will enhance understanding of an organization’s readiness status, and actions required to improve its responsiveness.
Chapter 5 – Conclusion and Implications

5.7 Concluding Remarks

This final chapter has reviewed the purpose of this study introduced in Chapter 1, highlighting the outcomes and responses for each research question, and confirmed a satisfactory achievement of the purpose of the study. This chapter has also described the major contributions to knowledge and implications of the outcome to the theory, policy, and practice of information risk management and action research, with suggestions for future research.

The substantive piezoelectric theory and the responsive strategy are the basic approaches developed in this action research study to resolve the issues and dilemmas of managing information risk in organizations faced with a constantly changing risk landscape. The study identified that change events, situation awareness, and critical alignment are three key elements that constitute responsiveness, and hence reflect the status of information security in organizations. These findings serve as a foundation for developing action strategies and implementing practical tools and processes for managing information risk, including both known and unknown (or unanticipated) risks, therefore enabling the organizations to be responsive to the changing risk environment.

The practice of action research throughout this study over the last five years has been a rewarding and beneficial experience, both in the intricacies of conducting an action research study, and as a study of my professional practice in information risk management, as a practitioner, as well as an advisor.

Being an engineer by training, with most of my early career focusing primarily on the technical aspects of information security, the social aspects of information security and its management were very much an unknown in my knowledge, sprinkled with pockets of experiences in dealing with people and groups in only the six to seven years prior to the study. While the industry has also started to step up on the importance of management in information security, as reviewed in Chapter 2, the approach from a social perspective has been quite limited. Through the study and use of action research methods, including reviewing the related literature, I have come to be more aware of the existing knowledge, issues, and dilemmas from a social-technical perspective. This, besides contributing to the outcomes of the study, has
helped me to look at information security management differently than I would have if continued on the more technical-oriented approach.

Being an action researcher has changed my way of thinking, in my being more open and reflexive in examining issues and evaluating actions, using critical reflection and always seeking for disconfirming evidence to validate against an hypothesis or a specific knowledge claim. The practice has also helped to improve my confidence in dealing with the unknowns (change events), and unexpected changes, given that the cyclical nature of action research will allow for understanding to be gained through the process, even though a situation may be fuzzy in the beginning. Practicing reflection-in-action has further improved my sensitivity (situation awareness) to issues arising and actions undertaken (including those of others), and at the same time being less reactive to the outcomes of those actions, focusing more on understanding the outcomes and issues involved, potential improvements and possible next steps of actions that might address the emerged issue (critical alignment), which helps to maintain calm and stability especially in situations in which such posture and mindset are more important than taking drastic reactive actions. Interestingly, these learning align with the key elements of responsiveness as developed in the study.

From a day-to-day practice perspective, journaling has now become a natural way for capturing my observations as and when data or event emerges. Besides helping in data retention, it supports my ongoing thinking and knowledge inquiry needs in my professional practice and research. Conversant in other methods such as dialectic analysis, and convergent interviewing have also enabled me to more systematically handle and sort through data of different contents or from people of different experiences.

Besides learning about action research and becoming an advocate, I have also learned much about information risk management from fellow practitioners who participated in this study. Their experience and knowledge had contributed substantially to this study and its outcomes, helping in the achievement of the purpose of this study. Managing information risks in a changing risk environment requires personal skills and dedication, and a passion for the subject matter, qualities that many of the research participants demonstrated during this study.
In closing, I have personally learned a great deal from this study, and I am sure the lessons, experiences, and knowledge gained will put me in a good stead in any future action research studies that I attempt.
Notes

1 The objectives of information security risk management may vary depending on the organization’s business, and also the regulatory requirements that it needed to be in compliant with. This was also found to be the case in different information security literature as reviewed in Section 2.2.

2 ALPHA was used instead of the company name to provide anonymity to the organization where this research was conducted. ALPHA was a multi-national financial institution with a presence in more than 50 countries internationally.

3 In ALPHA, the information risk management (IRM) function was established to identify and assess information security risks, and provide recommendations to the business for their treatment, which may be in the form of mitigation, avoidance, transfer, or acceptance measures. The IRM function was also involved in tracking the progress of implementation of the risk treatment measures that business has accepted, and manage any issues arising from the implementation.

4 Bangkok, Hong Kong, Jakarta, Kuala Lumpur, Manila, Mumbai, Seoul, Singapore, Sydney, Taipei, and Tokyo were the cities. Most information risk management activities were, however, focused in Hong Kong, Mumbai, Singapore, Sydney, and Tokyo.

5 For a thorough account of the 9/11 incident, see the published report of the 9/11 Commission – (Kean et al., 2004)

6 “Offshoring” was a term commonly used in businesses to refer to the transferring of business operations from a relatively mature site to a new site by leveraging the low infrastructure and human resources cost of the new site, normally located in a developing country such as India, the Philippines, and China. Unlike outsourcing, in which the operation was contracted out to a third-party provider, in offshoring, the operation continued to be owned and operated by staff of the business operation.

7 There was no universally agreed upon definition of SPAM, but, in general, it referred to unsolicited electronic messages that were sent in bulk by unknown senders, or senders with whom the recipients have no prior personal or business relationship.

8 According to Clark (2003, pp. 40-43), the Code Red virus cost the business community $2.6 billion; the Nimda worm infected close to 2.5 million servers and users worldwide in less than 24 hours; and the Melissa virus, which was unleashed by a New Jersey programmer in March 1999, caused at least $80 million in damages. ALPHA was not spared from these attacks.

9 The Information Risk Manager, or IRM Manager, was a member of the Information Risk Management (IRM) function, whose job was to perform the risk management tasks such as risk identification and assessment, and provide suitable recommendations, with justifications, to business management for risk treatments. At the regional level, the plans and activities of the IRM were managed by the Regional Information Risk Officer (RIRO) in the regional office. At the global level (across the entire ALPHA organization) the global Chief Information Risk Officer (CIRO) managed the global policies, strategic directions, and plans in the global office.


11 This issue has only been looked into in ISO/IEC JTC 1/SC 27 in 2006, with the development of the 2700x series of information security management systems related standards, including a new standard, ISO/IEC 27000, to capture all related vocabulary and terminologies, which was in Working Draft at the time of this writing.

12 “Information risk”, in the context of this project, is used in this dissertation to denote “information security risk.” In the industry, they have also been used interchangeably.

14 In 2005, the ISO standards committee (ISO/IEC JTC 1/SC 27) responsible for developing information security-related standards then began to look into developing international standards for measuring the effectiveness of information security management in organizations. There were,
however, many disagreements between standards experts from different national bodies on the terminology between measurements and metrics. At the same time, there was no specific method of measurement that standards experts could agree upon. A formal international standard is not expected until 2008 or later. This insight was gained through my personal participation in the capacity of Head of Delegation for the Singapore standards body in the ISO/IEC JTC 1/SC 27 meetings that were held every six months in various locations.

13 BETA was used instead of the name of the second company, a technology product provider, to maintain anonymity of the organization.

16 Information security risk was “dynamic” in that it was constantly changing along with technology use, people’s behaviors, and when risk management activities took place. As such, complete elimination of risk or security exposure was impossible.

17 In 2004, in ALPHA, the function was named as “information technology risk management” in order to ensure that it was focusing only on information technology related risks, but not information in general. In 2005, ALPHA had another change of leadership in the risk management function, and the group was named as “information technology control management” to emphasize the focus in the area of controls.

18 There was a slight distinction emerging between information security (but not information security risk) and information risk in the industry as some organizations (including ALPHA) were beginning to separate them into two functions, with the former focusing on the technical aspects of threats, vulnerabilities, and security solutions, and the latter focusing on devising and implementing a holistic framework to manage threats, vulnerabilities, and solutions involving the people, process, and technology used in the organization’s information systems and network. Information risk management was regarded in these organizations as a “new” risk management paradigm that an organization needed to focus upon just like managing market risk, settlement risk, and credit risk in a financial institution. The focus of this research was on the latter – information risk management—which is also referred to as “information security risk management” in the industry.

19 CHARLIE was used instead of the name of the company to provide anonymity to the organization that implemented an information security risk management approach that was derived from this research study.

20 Many regional and local organizations did not have an information security risk management function during the period of this study. In most cases, the IT department undertook this responsibility on a part time basis.

21 Existing baseline approach covered protective, detective, and recovery controls. Recovery was an after-event control. As such, organization might be able to recover from a failure or disaster, but unable to manage an emerging security situation that was materializing an information risk, even though new adverse security events have been detected through the detective controls.

22 “Piezo” is a Greek term that means “to squeeze.” When the piezoelectric elements, a type of electromagnetic material, are strained by an external force, say a squeeze or push occurred through an external event, they displace electrical charges accumulated on opposing surfaces. This has provided the elements with many practical applications.

23 Note that there were also substantial research and development in other areas of information security but were not directly related to the management aspects in business organizations. For examples; security engineering, trusted computing platform, and cryptography. All this has expanded the epistemology of information security.

24 OCTAVE™ was abbreviation of “Operationally Critical Threat, Asset, and Vulnerability Evaluation”. It was a risk evaluation methodology conceived at Carnegie Mellon University to define a systematic, organization-wide approach to evaluate information security risks. During the initial phase of this study, organization ALPHA has also evaluated OCTAVE™ for adoption and use as the company’s primary tool for information risk management. The tool was however not selected due to the complexity of the methodology and cost of implementation involved.

25 Appendix C provides a summary of the synthesis of the five forms of definitions against the common approaches for information security.
Dhillon and Backhouse suggested the addition of “responsibility”, “integrity” (as in reputation of a person), “trust”, and “ethicality”, as additional principles that information security management should include in order to address the challenges of new technology development and convergence, and the way work has evolved in the new millennium. These principles relate closely to the individuals acting in a business environment. As such, Dhillon and Backhouse focused their research on the social-organizational aspects of information security management.

It was also a common belief among some practitioners that if we can fix the security issues at the technology layer, those issues will be resolved.

BS 7799 was a two-part standards published by the British Standards Institute (BSI), providing guidance on “Code of Practice for Information Security Management” (BSI, 1999a), and “Information Security Management Systems” (BSI, 1999b). As of 2006, both documents have been withdrawn by BSI, and replaced by ISO/IEC 17799 (2005b) and ISO/IEC 27001 (2005c), respectively.

The cost of security is usually considered much later in the baseline approach, during the product or solution selection process, with the use of volume of purchase to negotiate with product or solution providers, or the use of a lowest-cost bidding approach to select the ultimate provider.

Risk identification involves identifying an asset and its associated value as the first step. If there is no asset to protect, there is no risk to assess and, therefore, to manage. In an information system, information has commonly been regarded as an asset. To protect information, the physical system involved, including the network, computer, storage media, and application software have also been regarded as assets, as their security affects that of the information processed, transmitted, or stored in the information system. The value of these information and physical assets varies from organization to organization. Over and above the monetary value involved, there are also other intangible assets such as an organization’s reputation or goodwill, which will be affected by the loss or unavailability of its information or physical assets. For each asset identified, the possibility of loss is assessed. The possibility of loss may result from deviation from the expected outcome or event, or the characteristics or properties of the assets involved. To assess this, the process of risk analysis has been used.

Risk treatment referred to the process of selection and implementation of measures to modify risk, including avoiding (or preventing), optimizing, transferring, and/or retaining risk. Risk acceptance referred to a decision to accept or retain a risk.

Risk communication was defined as “the exchange or sharing of information about risk between the decision-maker and other stakeholders” (ISO, 2001).

CRAMM was developed by the United Kingdom Government’s Central Computer and Telecommunication Agency (CCTA) and BIS Information Systems Ltd (BIS), London, UK, and released in 1988. CRAMM is an abbreviation for the CCTA Risk Analysis and Management Method.

RISKPAC was a commercially developed product of Chemical Bank Information Systems and Profile Analysis Corporation in the US. It provided a framework that can be loaded with set of questionnaires. Assessment was made using a scoring system as a measure of risk, which influenced the result of the analysis.

A term that was previously used in the building industry for testing the strength and reliability of core structures, “penetration testing”, in the IT industry refers to the use of hacking techniques to try and overcome the security protection of an IT infrastructure or systems, to look for security vulnerabilities as part of the risk assessment process.

The potential to cause harm or exploit a weakness is a threat to the system. If there’s no interest of anyone to cause harm to the system, there is no threat, and no attack (or exploitation) will be envisaged. In the context of an information system, common threats include unauthorized reading or disclosure, unauthorized writing or updating (forgery or corruption), and denial of service or access (making it unavailable when needed). Similarly, if there is no means to exploit vulnerability, an attack cannot occur as well. Although software and systems engineering have progressed over the past decades, many inherent properties of an information system cannot be completely predicted up-front. The complexity of information system lends itself to emergent behaviors that at times result in unintended vulnerabilities. It is therefore impossible to ensure that information systems are free from vulnerability. At best, we can only eliminate weaknesses known from past experiences with similar systems.
Vulnerability is commonly referred to as a flaw or weakness in a system (which may be in the hardware, software, or procedure) that enables security breaches. Unlike other functional features of a system, vulnerabilities are often hidden, even unknown to the designer, or can be part of a feature of a system. This therefore makes its identification and assessment at odds with the objective of risk assessment.

The Integrated Business Risk Management Framework was essentially justified based on the same premise as in (Blakley et al., 2001) The approach regards information security and technology-related risk as one of the many business risks, and focuses on bottom-line business impact, or value added, instead of risk modeling.

Scenario Analysis Approaches involved the construction of different scenarios by which computer security may be compromised, to illustrate how vulnerable an organization was to information attacks. Also used to encourage broader brainstorming about computer-related risks to demonstrate the variety and severity of risks faced. The scenarios deemed most likely and of greatest severity were then used as the basis for developing a risk-mitigation strategy (Hoo, 2000).

In practice, risk management co-ordinates the activities of risk assessment, risk treatment, risk acceptance (or retention), and risk communications. It is important to evaluate risk management at the appropriate level; effective risk treatment itself does not guarantee effective risk management. For example, failure in risk communication can result in negative perception of the organization, with other risky consequences, even though that the organization might have taken the most appropriate measures to treat the risks that have been identified and evaluated accurately.

In commercial businesses, liability may be transferred by disclaimer or agreement. The former involves undertaking activity with the explicit understanding that the organization will not be held responsible for the consequences of certain adverse events, but without specifying who will be responsible for those consequences. The latter arises from entering into an agreement with a different party to take responsibility for the consequences of certain adverse actions.

Indemnification is commonly carried out through pooling or hedging the risks. Pooling occurs through the sharing of the cost of certain risks by several businesses, on the assumption that adverse events are unlikely to happen simultaneously to a meaningful fraction of the organizations in the pool. Insurance policies are the most common risk-pooling scheme; they increase the predictability of the cost of risk, and at the same time decrease the cost of risk for each organization in the pool. Hedging involves betting on the odds of the risk not occurring, which essentially capitalizes on risks to make money.

“Adverse selection” refers to the potential of the insured knowing certain risks but not reporting them to the insurer.

“Moral hazard” refers to the lack of incentives by the insured to take actions that reduce the probability of a loss subsequent to purchasing the insurance.

Insurance companies will typically be concerned about the issue of adverse selection when offering an insurance policy. Organizations that do not understand their own risk profile will be assessed as a higher risk than those that do. On the other hand, organizations that understand their own risk profile may know of certain risks and keep them from the insurance company in order not to pay higher premiums for their policies.

According to the E&Y report, the 2005 survey covered 1,300 respondents from 55 countries (Ernst & Young LLP, 2005).

LeVegue’s (2006) contribution in the information security strategy literature was only fairly recent, and was focusing mainly on the methodology and processes for developing a strategy, rather than specific strategic approaches for addressing information security issues and dilemmas relating to the context of this and other similar studies.

“Information warfare” involves identifying the information needs of the potential attackers, or competitors (in the case of a business), and taking measures to control information flow to the potential attackers or competitors. The controls may range from the creation of false information to the sanitization of information, with the objective of confusing, misleading, or simply so that the attacker or competitor cannot act positively to their advantage.
"Bounty program" involves establishing a reward system to promote "whistle blowing" about known perpetrators, so that the victim organization and/or law enforcement can take legal action to stop future attacks.

Timeliness was also one of the nine principles recommended in the OECD’s "Guidelines for the Security of Information Systems" (OECD, 1992). In 2002, this principle was replaced with the "Response" principle.

The approaches may be information risk management, baseline security, use of security technology, or a combination of these principle-based approaches. In practice, organizations may (and are likely to) use a combination of approaches to address different needs and compensate for the lacks in each approach. All three approaches are therefore used in most organizations.

The CISSP certification scheme is managed and promoted by the International Institute of Systems Security Certification Consortium, or (ISC)^2. For more information about CISSP and (ISC)^2, see also (ISC)^2 web site at [http://www.isc2.org/](http://www.isc2.org/).

In the context of information security risk management, an example of a broadly applied policy may be "use of all network access points will be logged and monitored"; an indication of normal practice may be "company policy is to use local security consultants for risk assessment"; and a specific commitment may be "there has been a policy decision to phase out the use of passwords for all business applications in two years".

These weaknesses are normally unintentionally left out or ignored by risk managers or IT auditors, but due to differences of opinions about their significance or knowledge of their existence at the point of assessment.

In the IT industry, reporting vulnerability publicly without first addressing with the technology provider is highly discouraged, since this exposes the end-user systems to a higher possibility of attack. Most vendors therefore promote the concept of responsible disclosure, based on a published guideline, entitled "Guidelines for Security Vulnerability Reporting and Response Process – V2.0", by the Organization for Internet Safety ([http://www.oisafety.org/](http://www.oisafety.org/)), for both the vulnerability finder and the vendor involved to follow, to ensure end-user systems security without aiding the potential perpetrator.

The Center for Information Systems Security Studies and Research (CISR) is one of the centers for military research and education in Information Assurance (IA), defensive information warfare, and computer and network security. More information on CISR is available at [http://cisr.nps.navy.mil/index.htm](http://cisr.nps.navy.mil/index.htm), last accessed on March 25, 2006.

The concept of responsibilities in security include "ownership", "custodianship", "control", "system user", and "accounting". For more details on these concepts, see Dorey (1994, pp. 27-74)

"Known risk issues" refers to information risks that are known within the organization.

For example, an exploit that worked in the past may not work in the current moment due to technology changes, resulting in elimination of the targeted vulnerability, or simply incompatible techniques involved.

As in the definition of validity, Greenwood and Levin (1998, pp. 80-85) distinguished between "internal" and "external credibility". "Internal credibility" refers to the direct impact or consequences of the research outcomes in altering the patterns of social actions. "External credibility" refers to the aspect of the "knowledge capable of convincing someone who did not participate in the inquiry that the results are believable".

Glesne (1999, pp. 32-33) suggested (1) prolonged engagement and persistent observation; (2) triangulation; (3) peer review and debriefing; (4) negative case analysis; (5) clarification of researcher bias; (6) member checking; (7) rich, thick description; and (8) external audit” as eight methods of verification for validity. The purpose of "prolonged engagement and persistent observation" is to use extended time in the field to develop a trust relationship with the participants/stakeholders, and understand the culture, thereby facilitate more truthful and objective feedback from the participants/stakeholders. The iterative nature of action research integrates such a procedure in the methodology. "Triangulation" refers to the use of multiple sources of data and data collection methods, engaging multiple investigators, and/or taking multiple theoretical perspectives on the data. "Negative case analysis" refers to the conscious search for negative cases to provide disconfirming evidence in
order to refine the working hypothesis underlying the study. “Rich, thick description” refers to the documentation of the observations and other research data in such a way that allows the reader to enter the research context. “Rich, thick description” refers to the documentation of the observations and other research data in such a way that allows the reader to enter the research context. “External audit” refers to engaging an external person to examine the research process used, through checking the field notes, journals, and any coding scheme used.

62 Negative case analysis refers to a method of validation that involves seeking evidence from new data and previously collected data to disconfirm a hypothesis, and reformulating the hypothesis thereafter when disconfirming evidence is found. The process is repeated until no more errors can be found to disconfirm the latest revision of the hypothesis formulated from the fact.

63 “Ideographic” refers to “an approach to social science that emphasizes that explanation of human behavior is possible only through gaining access to actors’ subjectivity or culture” (Gill & Johnson, 2002, p. 227).

64 “Nomothetic” refers to “approaches to social science that seek to construct a deductively tested set of general theories that explain and predict human behavior” (Gill & Johnson, 2002, p. 228).

65 “Co-option” refers to a working relationship between two parties that is one directional such that one party is the provider and the other, the recipient or dependent of the services provided.

66 A “dialogical view” is one where the relationship between participants and researchers which, through the use of dialogues, open communicative space to promote a critical consciousness, permitting people to achieve mutual understanding and consensus. Such a relationship is exhibited by the political and practical actions taken to promote change as a result of the understanding and consensus achieved.

67 “Firm” is the term used within ALPHA to denote the company. It is used interchangeably in this report with the words “organization” and “company”.

68 The “Aristotle Table of Invention” is a structured approach for finding the thematic concerns, or identifying possible answers to an already-identified thematic concerns, using a N columns by N rows table by working through a series of questions through each cell intersected by each column and row progressively. N is determined by the systems involved, which includes the key stakeholders, the subject matter of concerns, and the contexts of the situations assessed. For example of its use, see Kemmis & McTaggart (1988, pp. 91-99).

69 ALPHA was a merger of more than three major financial institutions in between year 2000 and 2002. As such, there were several information systems and databases, each used by respective pre-merger firm to archive and share information in the company. “Heritage organization” refers to the respective firm prior to the merger with ALPHA.

70 Note that all research journals are indexed by the date of creation and with the prefix “J”. See appendix for the list of journals in the register.

71 The term “Asia” is used quite loosely in the company, which actually includes Australia and New Zealand. However, there were no significant IRM activities in New Zealand since it was supported by Australia (staff in Sydney.) My data collection process included interviewing of stakeholders in Sydney as well as Singapore, Hong Kong, and Tokyo.

72 The activities of Asia IRM team members had direct impact on other stakeholders’ perception and results on IRM deliverables and future development. In addition, IRM’s practice, ongoing business support and future function and focus will be affected by stakeholders’ acceptance of IRM deliverables and perception of IRM’s value contributions.

73 The Global Corporate IRM determines the main direction and agenda for the IRM team in the company, and hence having impact on my plan and also provided a channel for escalation of issues from the region.

74 Asia did not have dedicated IRM for business lines as resources in the region were shared across business lines then.
One may argue that such attitude of the stakeholders could be due to a lack of information security risk awareness, and by improving awareness, priority for information risk activities will escalate. While education and awareness may help, they do not replace the individuals’ and groups’ immediate, shorter terms goals and agenda. The effect of education and awareness is often long term. It is therefore essential to look at other approaches to bring information risk considerations and activities into the stakeholders’ agenda, instead of simply relying on education and awareness. Having said this, education and awareness were also incorporated as part of the IRM Program throughout this study, in view of the importance of such activities in bringing about longer term cultural and practice changes.

External from the perspective of IRM organization, i.e., they were not member of IRM organization. However, they were not external member (staff) of the organization as a whole.

Operational risk capital (ORC) provision was an amount of funds that an organization (financial institutions) has to set aside annually so that in the event of the realization of any operational risks affecting the organization, the funds can be used to cover the losses incurred. ORC was catered for only operational risk issues, which included systems (and information) risks. It was computed based on the operational risk managers’ assessment of the potential exposures (or risk) that the organization faces. The audit result (rating) was used as a factor on this capital provision, since it should demonstrate how well the controls were in practice in the organization to manage those exposures/risks. In the case of organization ALPHA, the factors were 0.85, 1.00, 1.25, 1.5, and 2.00 for rating of ‘A’, ‘B’, ‘C’, ‘D’ and ‘F’, respectively. If a department has a ‘C’ or lower audit rating, their operating budget for the year will be reduced by the equivalent percentage based on the ORC factor. For example, if the ORC was computed at USD 1 million, a ‘C’ rating for the department would bring it up to USD 1.25 million. This would normally translate into further cost cutting, reduction or elimination of bonuses, or even retrenchment of staff, in order to provide for the ORC adjustment required. On the contrary, if the department has achieved an ‘A’ audit rating, the ORC would be reduced by 15%, translating into additional budget for operations, bonuses, etc. As such, audit rating became a key motivator to be compliant.

As the organization was a merger of three major financial institutions and several smaller Firms from different parts of the world, one of the exercise undertaken prior to merger was identification of “control gaps” that existed in each heritage organization, using the newly updated (as of August 2001) IT Control Policy as a baseline. The gap remediation project was initiated to close the top ten gaps identified. However, those control gaps were identified through a sampling approach (not comprehensive review), prior to the merger. Their validity post merger have not been verified at the time of this study, and indeed was not verified when the gap remediation project was formally launched in mid-2002. The global gap remediation project was poised to resolve the top ten security issues facing the newly merged organization.

Control self assessment (CSA) was a process designed and directed by the Operational Risk Management (ORM) department, which included information risk as one of the component for assessment. It was a checklist-based process requiring the business manager for each department to go through on a half-yearly basis to identify any missing controls or potential control issues in their scope of business. The results were then input to a central database system whereby periodic reports were generated for management to have a comprehensive view of the status of the business systems from a control perspective. For every checklist question that had been completed, it was marked as “green”, “amber”, or “red”, in accordance to the status of compliance, i.e., comply, action is being done to comply but not fully implemented yet, and not complied and no planned action yet, respectively. CSA was not a process peculiar to organization ALPHA practices, but a common tool used by ORM, and also Central Banks in numerous countries to ensure that the financial institutions practice some form of risk management and controls in their organization.

If an issue was identified by the auditor but not captured as one in the CSA report, the business department may also receive a poor audit rating for failing to perform a thorough or accurate self-assessment.

In one of the heritage (see note 78) Firms, IRM was organized as a “business aligned” function, reporting directly to business manager (or business application development manager) and her main task was to handle the CSA and audit related activities. In another heritage organization, where the R&C function was practiced, IRM focused only on providing technical security advices for addressing control issues. However, IRM was also engaged by the R&C function to assist in conducting security
reviews (known as “pre-audit review”) a few weeks prior to major audit schedule in the business to ensure that any control issues were addressed prior to the audit. During the audit process, IRM will also perform the audit coordination function.

82 A check of the knowledge background, training, and experience of existing IRM managers revealed that more than 50% of the staff did not have an information security or risk management qualification, training, or job experience prior to joining the team. They were mostly project managers or auditors before being transferred to the IRM position.

83 To understand the extent of the security risk management issues and dilemmas in BETA’s customers’ organizations (which included government, financial institutions, and other business enterprises), I designed a mini-survey comprised of 37 questions and used it as a basis for further data collection with the stakeholders in those organizations. The survey questionnaires were used to guide a series of structured interviews with 30 respondents, to determine the similarity and differences of their security risk management challenges, and their strategy and plans in managing those issues and dilemmas involved. The interviews and responses collected from the survey provided new insights on the issues and dilemmas in information security risk management.

84 In one of the heritage organizations, IRM functioned as part of the business organization, and it was known as Business-aligned IRM (BIRM). In this approach, the IRM reports into either the Head of Operations, or the Head of Business Application Development, and her cost was fully absorbed by the business. BIRM itself is a global organization within the business organization. For example, in the Investment Banking business, there was a global BIRM team, and in each region and business center in a strategic geographic location, there is a local BIRM team supporting those regions /centers locally. BIRM only served her own business department. In other words, an IRM from the Investment Banking business would not do work for the Retail Bank, and vice versa. This ensured business specialization and focus for IRM.

85 In another heritage organization, IRM was part of IT Services, and grouped as a centralized, shared pool of resources to serve all businesses. In terms of funding the resources, the businesses were charged at the end of the year based on the actual utilization of the IRM. The funds were pre-allocated based on previous year utilization. This model enabled better scalability and a greater variety of work for the IRM members. On the other hand, there was no business specialization. IRM was required to understand the information risk issues in all the businesses that she managed.

86 In the newly merged organization, a pooled resource model was adopted with a slight modification. An IRM team was established to focus on helping the businesses manage their information risks, and a team of security engineers was established to support IT Services in infrastructure security and business application development teams in application security risk management. In terms of reporting structure, the regional team has two lines of reporting, one to the regional Head of IT Services, and another to the region’s Chief Operating Officer (COO). The Global CIRO’s rationale for this reporting was to ensure a balance of power, and allow for business issues escalation to the COO whenever necessary.

87 In organization ALPHA, regional centers include Singapore, Hong Kong, Tokyo, Sydney, and Mumbai.

88 The Location Operating Committee (LOC) was set up in each operating location in the region to monitor and address all operation-related issues in the country. This included information security risk issues that were found in the systems used by the lines-of-business in the location. The LOC was chaired by the Head of Business Operations of one of the lines-of-business. Its members included all the Chief Control Officers (CCO) of each line-of-business, the Head of Compliance, Head of Audit, Head of IT Services, and respective Head of Business Application Development for that location. Its agenda also included regulatory and compliance issues and requirements.

89 This risk did not materialize as the COO did not take on an active interest in managing the regional IRM function. On the other hand, the COO has agenda items that require assistance from IT Services, and therefore preferred to let the Head of IT Services continue to be the primary reporting line for IRM in the region. This effectively made the parallel reporting redundant.

90 The Simple Network Management Protocol (SNMP) is a network management protocol that is part of the Internet protocol suite, for devices and computer systems on a network to provide status of their
well being and configurations to a requesting station in a standardized manner. Weakness or vulnerabilities on SNMP could potentially result in a perpetrator gaining information on device configurations, which would allow him/her to compromise the security of information and systems on the network.

93 SPAM refers unsolicited electronic mail messages, normally sent by advertisers and marketers to solicit recipients’ visits to their web sites, or the purchase of products. In 2002, they were mainly an annoyance to the recipients, as they quickly filled up users’ mailbox, and took time to be removed. In 2003, they began to carry malicious programs that often tried to take control or steal data from users’ machines, including sensitive business and personal information (The Economist, 2003).

92 In the NIST Risk Management Guide for IT Systems (Stoneburner et al., 2002), there were nine steps in the risk assessment process. The first step involves systems characterization, which can be grouped as part of the asset identification step. The threat and vulnerabilities analysis steps were separated into two steps, and additional steps on countermeasures, control analysis and results documentation were also suggested. In essence, they encompassed the four steps described in this section.

93 Knowles categorized the criticality of risks identified into three levels of “materiality”, namely, “group materiality”, “Strategic Business Unit (SBU) materiality”, and “low materiality”.

94 Adopted from organization BETA’s internal document.

95 The problem is asymmetric as we do not know what the potential attackers already know, but the potential attackers can find out what we know, since our methods are open, and often based on common or standard practices and available technology solutions.

96 Hurricane Katrina was a disaster that struck New Orleans and the Gulf Coasts areas of the United States as a Category 4 (and at one point up to Category 5) hurricane in late August 2005, killing tens of thousands of people, destroying infrastructures, and leaving many more homeless.

97 Malware is generally used as a short form of the phrase “malicious software”, which means software programs that have a malicious intention encoded within them that could potentially harm the users or organization using the programs.

98 The Organization for Internet Safety (http://www.oi-safety.org/) is one such organization established by various technology vendors to promote the principles and practices of responsible disclosure.

99 This implies a need to reconsider IRM, business continuity and disaster recovery planning function and organization, as discussed in Section 4.3.4. Details of the events involved and the analysis conducted are documented in research journal J20061126.

100 The outcome of this analysis was published in the Journal of Professional Information Security Association (PISA), Hong Kong (Kang, 2005c).

101 The dotted (red) lines show a negative influence along the direction of the arrow head. The solid (blue) lines show a positive influence. The plus (+) and minus (-) signs at the beginning and end points of each arrow show the respective increase and decrease of each point in the system. For example, an increase (+) in undesirable behavior would lead to an increase (+) in the number of weak systems, and vice versa; but an increase (+) in education activities would lead to a decrease (-) in undesirable behavior and, consequently, a decrease in the number of weak systems.

102 Risk Acceptance, commonly known in organization ALPHA as RA, was a process formally documented in the IT Control Policies to permit the Information Owner to accept the risk identified, under specific conditions. The conditions included the requirement for the risk to be formally documented, and the cost and resources for mitigating the risk was assessed to be too high for the risk involved. In addition, it required compensating control procedures (using manual means) to be implemented to minimize the possibility of exposure to the risk involved. In practice, however, RA was found to be misused frequently to bypass control measures that were either too time consuming, or difficult to comply with. For example, in an incident recorded in J20020430 and J20020510, the request for a Generic ID required for application access to database systems was preceded by the submission of a RA form in which the issuer (from the IT department) could account for the issuance without the need to validate the necessity of the request. This was clearly a misuse of the procedure. A subsidiary project was initiated to subsequently eliminate this practice.
This analysis and the series of systemic diagrams were also used as part of a set of tools for explaining the benefits of the IRM program to the stakeholders.

An example of such control issues included legacy application systems’ non-compliance with security settings required by the IT Control Policy, such as non-compliance with minimum password length. To gain compliance, either the legacy application needed to be replaced, or custom-built security systems needed to be developed. Both options were costly and unjustifiable from a business point of view. Such an issue therefore requires a risk decision to be made.

The ISRA process, which was documented as part of organization ALPHA’s IT Control Policies requirements, involves identification of information assets (including application systems), business owners, classification of assets, and a higher level assessment of the potential threats and impacts of those assets.

The IRM scorecard was a two-dimensional table with the Y-axis listing all the required controls as specified in the IT Control Policies, and the Y-axis listing the LOBs and core infrastructure system components of the organization (in ALPHA). Each cell in the table reflected the status of compliance, of LOB unit, or infrastructure component, with the required control, in either Green (fully compliant), Amber (partially compliant), or Red (not compliant).

A comprehensive review of the literature in this area has been conducted and discussed in Section 2.5.4.

Details of the changes involved were annotated and analyzed in research journal J20060826.

This phenomenon was also discovered in social situations relating to the movement of people, as noted in Schelling, cited in Robert Dodge (2006, pp. 129-144).

An adversary refers to anyone whose actions could result in the realization of a security threat to the organization. The initial outcome of an adversary’s action is the emergence of a security event, which may or may not be obvious, and may result in a security incident.

Scenario planning was however not used in organization BETA for the readiness preparation. The testing efforts in organization BETA were focused on validating the data collected. Actual actions were spelt out in the security messages (for example, alert emails) to instruct individuals of their responsibilities and actions required during the incident itself.

Criticality, in Knowles’ context, was a term used to state the significance of an information security risk to the organization in order to bring attention and resources to manage it. Similarly, the idea of criticality as used in organization BETA’s approach for managing emerging risk was to indicate the seriousness or significance of a security event that have the potential to unfold into an incident. In those approaches, criticality is risk focused, but not necessarily business aligned. Furthermore, the materiality and significance of risk are still subjective, dependent on the risk analyst assessing it, regardless of the actual terminology used.

Business continuity and disaster recovery were identified as a criticality alignment requirement for Singapore from both risk and opportunity perspectives due to the aftermath experiences and learning of the SARS epidemic, and also the September 11, 2001 incident, in which both had negatively impacted Singapore’s economy for a period of time.

See Sections 2.3.6.1 and 4.2.7 for discussion on other limitations, such as subjectivity, a general lack of consistency, and a focus on mitigation.

Japan Telecom-ISAC is a consortium of major Internet Service Providers (ISP) in Japan, established for the purpose of information sharing and analysis (ISAC), on security events and incidents on the ISP networks in the country. More information about the consortium can be found at https://www.telecom-isac.jp/about/index.html.

The text in parenthesis was based on verbal clarification with Koji Nakao in a meeting held on November 3, 2006 in Singapore. The meeting also confirmed the accuracy of the incident related information, and validity of the analysis conducted.
For examples, existing literature such as Mandia, Prosise and Pepe (2001), and international standards ISO/IEC 18044 (ISO/IEC, 2006), that provide guidance on incident response mostly focused on establishing a process in preparation for collecting evidence and investigation activities.

For details of the Internet Storm Center operate by the SANS Institute, visit its online web site at http://www.sans.org/.

For details on SANS Institute, see http://www.sans.org/.

The aim of the review should be to learn from the failure rather than to find a scapegoat to bear the consequences. However, individuals may feel guilty for their actions and therefore change their statements in order to protect themselves from the responsibility.

A poorly-designed plan or action strategy, in this context, referred to one that lacked the essential elements and input required of a responsive strategy. For example, not considering the input and elements as depicted in Figure 30.

Badly executed actions could be in many different forms, such as a lack of coordination, no prior training and/or lack of information dissemination to ensure participants awareness and competence to execute the desired actions.

Weak links (or security vulnerabilities) may be residual in the systems due to inadequacies of the risk assessment methods used, or emergence behavior resulting from the complexity of a “defense in depth” implementation. Adversaries exploit weak links in order to achieve their objective of materializing security threats to the organization.

Another approach that some information risk managers have adopted was to estimate the savings resulting from incidents that did not result in significant impacts. This approach is also subjective as there is no correlation between the actions of IRM and the non-occurrence of an impact, which is non-existence in the first place. Such an estimate is therefore questionable by business management as a method to measure IRM performance.

Two major limitations are time and accessibility to resources for development and implementation of such a measurement system, which by itself justifies a separate project. It is therefore proposed as a project for future research, as a sub-project to derive the formal piezoelectric theory of information security risk management.

“SECD4” is an acronym derived from the application of the five main applied social science methods in the social-technical process developed for social interaction in operating the information risk management system. They are: stakeholder analysis (S); entry and contracting processes (E); convergent interviewing (C); dialectic data analysis (D); and Flood’s (1999) Four-windows systemic view (4).

The RAISS Forum is a regional gathering of information security standards professionals in the Asia Pacific region, which meets half-yearly to provide updates on information security standards and information security-related issues and developments in each member economy. The Forum’s proceedings are published in print and online, available at http://www.itsc.org.sg/standards_news/raiss.html. The 5th meeting was held in Tokyo, Japan, on October 4th and 5th, 2006.
Appendices

Appendix A: Survey Questionnaires
Appendix B: Research Log Register
Appendix C: Synthesis of information security approaches based on definition used
Appendix D: Framework for Information Risk Management
Appendix A: Survey Questionnaires

Information Security Practice Survey

Introduction

This survey forms part of a research work being undertaken to study current information security practice and risk management in organizations. We are interested in seeking your responses to a number of questions about these practices.

Objectives

The objective of this survey is to gain an understanding of current organizations and practices of IT security management in enterprises and governments in the Asia Pacific region, and their focus in terms of their security policy, strategy, and plans in addressing IT security issues in organization.

Scope

The survey covers six areas, namely:

a. Background information relating respondent's organization
b. Security organization
c. Security policy
d. IT security function in security incident situation
e. Experiences in security incident
f. General view on IT security practices

Privacy and Confidentiality Information

No personal information relating to the respondent will be collected and stored as part of this study. In addition, report(s) resulting from this survey will be based on aggregated data from at least five respondent's input. If there's less than five responses received, the survey would either be extended until at least five responses are received, or discontinued. (we need to talk about this-if you only intend on surveying 5 people why not interview them?)

Respondents are advised not to provide any information that is deemed as confidential to your organizations. In any case, no organization-specific information would be published as part of the results of this survey or overall research work undertaken.

Freedom of Consent

If you decide not to participate in this survey, you are free to do so. By responding to the questions below, we assume that you have given your consent for the use of these information (in aggregated form) to participate in this research work.

The questionnaire will take approximately 45 minutes to complete.

Inquiries

Should you have any questions or concerns regarding this survey, please do not hesitate to contact the researcher: mengchow@acm.org.

Survey Questionnaires

A. Background of Respondent’s Organization

We need to get details of respondents such as age, position, gender
1. How would you classify your organization?
   - Financial industry
   - Manufacturing & logistics
   - Government
   - Technology systems integrator
   - Security services provider
   - Software
   - Hardware
   - Healthcare
   - Telecommunications
   - Transportation
   - Others (please specify):

2. What is the size of your organization?
   - Less than 50 staff
   - 50 to 200 staff
   - 201 to 1000 staff
   - 1001 to 10000 staff
   - More than 10000 staff

3. What is the geographical spread of your organization?
   a. Local company in one country _____ only (state country)
   b. Regional company in ____ Asian countries (state number)
   c. Global company in ____ countries (state number)

4. What’s your role in the organization?
   - Chief Security Officer or equivalent
   - CEO/CIO/COO/CTO or equivalent
   - Chief Privacy Officer or equivalent
   - IT/IS Manager or equivalent
   - Systems Administrator/IT Analyst
   - IT Security Consultant or equivalent
   - Others, please specify:

B. Security Organization
5. Does your organization have a dedicated IT Security Function/Department?
   - Yes
   - No. Please indicate how IT security activities are executed, and by whom in space provided below.

6. What is the title of the Head of IT Security?
   - Please specify:
   - Not applicable

7. Who does the Head of IT Security (or equivalent manager) report into?
- CiO or equivalent (will the respondent understand these acronyms?)
- CTO or equivalent
- CEO or equivalent
- Chief Operating Officer/President or equivalent
- Business Head
- CFO or equivalent
- Others, please specify:
- Not applicable

8. Does the Head of IT Security have a background working on Information Security for a number of years before taking this role?
- Yes
- No, please specify background
- Don’t know
- Not applicable

9. How many full time staff is in the IT Security Department?
- Less than 10
- Between 10 and 20
- Between 21 and 50
- Between 51 and 100
- More than 100, please specify:
- Not applicable

10. How many part-time staff is working for the IT Security Department (part-time means the staff is also undertaking other roles in the organization)
- Less than 10
- Between 10 and 20
- Between 21 and 50
- More than 100, please specify:
- Not applicable

11. How many of your IT security staff are CISSP certified?
- All of them
- Minority – 10% or less
- Around 50%
- More than 50%
- None of them

12. Does majority of your IT security staff have formal security training?
- Yes
- No

C. Security Policy
13. Does your organization has a formal IT security policy?
- Yes
- No

14. Does your organization adopt a risk management strategy to determine what to protect?
- Yes
- No, please describe approach taken to determine priority and budget for security:
15. It yes, who conducts the risk assessment?
- IT Auditor
- IT Security staff
- IT or Operation Risk Manager
- IT Manager
- Business Manager
- Others, please specify:

16. If risk assessment is undertaken, who affirms the results of assessments?
- Head of IT Security Department
- Business Head
- CxO whom IT Security Department reports into
- CxO whom Business Heads report into
- Others, please specify:

17. Does your organization have an IT Security Steering Committee or equivalent to determine policies and risk decisions?
- Yes
- No

18. Is your organization's IT security policy and practice in accord with ISO 17799-1 standards?
- Yes
- No (self developed)
- No (based on other standards), please specify standards used:
- No (hybrid of several standards), please specify standards used:
- Not sure

19. Is there a Security Plan or Program that the IT Security Department owns and executes?
- Yes
- No

20. What's the content of your Security Plan? (Please mark relevant items, number 1 to 8, 1 being most important)
- Security awareness program
- Security technology/project initiatives implementation
- Security review/testing program (on existing systems)
- Incident response and handling plans implementation
- Security monitoring activities/programs
- Conduct of security incident drills
- Disaster recovery planning and testing
- All of the above (equal importance)
- Others, please specify
- Not applicable (if you don’t have a security plan or program)

21. How would you classify your IT Security Strategy based on the following categories?
- Defensive security – main prevention and controls to minimize risk
- Reactive Security – main focus on incident response
- Recovery security – main focus on business continuity and disaster recovery
- Combination: Defensive [ ] %; Reactive [ ] %; Recovery [ ] %
22. What’s the main driver in your organization for implementing IT security? (Please mark relevant, number 1 to 7, 1 being most important)

☐ We need to address the virus/worms threats that are the key concerns of management and/or customers
☐ We know that there are hackers or fraudsters that will fraud our systems for financial gains or competitive reasons
☐ We need IT security to keep our systems available for our business and/or customers
☐ We need IT security to comply with laws and regulations that govern our business
☐ We need IT security to pass our annual audits
☐ We need IT Security because it is part and parcel of good business practices, just like finance and accounting
☐ Others, please specify:

23. What’s your main concern in implementing your Security Plan? (Please indicate the order of importance, 1 being most important, 6 being the least important)

☐ Insufficient budget or unable to justify required budget to management
☐ Don’t have the people who have the right skills to implement it
☐ Plan is incomplete, not addressing all issues
☐ Insufficient or no senior management support or commitment
☐ Plan is focusing on compliance rather than actual risks
☐ Other concerns, please specify:

24. What if your Security Plan were to lag behind schedule? (Please mark relevant items, in order of relevance, 1 being most relevant, 6 being most irrelevant)

☐ I’ll be fired, someone could take over to try it again, no significant impact to the business
☐ The business might incur financial losses or reputation damages due to fraud and attacks that exploits our system’s security weakness
☐ Our customers will get to find out about our system’s weakness and this will have a negative impact on our business
☐ The company will incur a regulatory/audit compliance issue, we need regulator/auditor’s approval to extend the schedule
☐ We will have to revise the plan to make it more achievable next quarter/period, but no major impact to business foreseeable
☐ Other consequences:

D. IT Security Function in Security Incident Situations

25. What’s the role of IT Security Function should an emerging security incident (or attack) be detected, but no failure occur yet? (Please tick all relevant answers.)

☐ No role specified for such situation
☐ Organize core team to monitor situation closely, alert relevant parties to get ready
☐ Organize core team to monitor situation, alert relevant parties when the situation deteriorate. Otherwise, stay put.
☐ Notify IT department to monitor situation and alert relevant parties. IT department takes over to make sure infrastructure is available
☐ Notify Crisis Management team to take over monitoring and determine actions
☐ Take preventive actions as appropriate
☐ Report to law enforcement when failure is confirmed
Obtain IT vendor support to help in identifying perpetrator or troublemaker
Acquire Security Consultants from eternal provider to help investigate situation
Others, please specify:

26. What’s the role of IT Security Function when a security incident (or attack) has occurred, system failure or compromise confirmed? (Please tick all relevant items.)

- Activate crisis management team to handle the incident
- Hand over incident management to crisis management team or equivalent
- Try to block perpetrator access with best efforts
- Ask for vendor (and/or security provider) assistance to block perpetrator
- Recover attacked systems back to production state
- Report (what do you mean by recover?) to law enforcement agency
Others, please specify:

27. What’s the role of IT Security Function after a security incident? (Please tick all relevant items.)

- Assist Audit or other function in investigation of incident to establish what went wrong and what needs improvement
- Take lead of the investigation of incident, same objective as above
- Fix the security discrepancies on the compromised systems using IT security department staff
- Organize/coordinate for third party to fix the security discrepancies on the compromised systems
- Let crisis management team decides what to do next and support as necessary
- Review security plans, policies, and infrastructure to determine improvements needed
Others, please specify

28. How prepared is your IT security staff to respond to a security incident?

- Well prepared, we have regular drills at least twice a year
- Somewhat prepared, we have a plan and it has been drilled before, though not regularly
- Some what prepared, we have a plan established to respond to security incident
- Not sure, we are still working on a plan
- Not prepared, we have a plan but not tested
- Not sure, we don’t have a plan yet
- Not prepared, we don’t have a plan yet

29. How prepared is the rest of your employees (not IT security staff) to respond to a security incident?

- Well prepared, we have regular drills at least twice a year
- Somewhat prepared, we have a plan and it has been drilled before, though not regularly
- Some what prepared, we have a plan established to respond to security incident
- Not sure, we are still working on a plan
- Not prepared, we have a plan but not tested
- Not sure, we don’t have a plan yet
- Not prepared, we don’t have a plan yet

E. Experiences in IT Security Incidents

30. Does your organization have history of computer related frauds?
31. If yes, were IT Security function involved in the investigation?
   - Yes
   - No
   - Not sure

32. Were your organization affected by the following worms/viruses previously? (Please mark relevant one, indicating level of severity (1 to 5) involved, 1 being most severely hit. Please mark only those that you have been affected.)
   - Nimda/Code Red virus
   - SQL Slammer
   - Blaster
   - Sasser
   - Netsky
   - Others, please specify
   - Never affected by viruses/worms in a significant way before (significant being defined here as more than 5 machines affected in one occurrence)

33. What was the role of IT Security function in the virus/worm incidents? (Please tick all relevant items.)
   - Source for anti-virus remedy (patches, updates, etc)
   - Install updates for users and servers to eradicate the virus/worm
   - Hand over updates to IT function to provide installation support to users/servers & eradicate
   - Investigate cause of viruses/worms and report to management
   - Investigate damages caused by viruses/worms and report to management
   - Review policy changes and other remedial activities required to prevent recurrence
   - Let IT function to manage and eradicate the virus/worms
   - Let IT function investigate and report the causes and damages incurred
   - Monitor for recurrences
   - Let IT function handle any post incident activities required
   - No prior experience to provide responses
   - Others, please specify

F. General Views on IT Security Practices
34. Should IT Security function combine with Business Continuity and Disaster Recovery functions as on single integrated function?
   - Yes, only IT security and business continuity
   - Yes, only IT security and disaster recovery
   - No, IT security stands on its own, business continuity combines with disaster recovery
   - No, IT security stands on its own, similar for business continuity, and disaster recovery
   - Other suggestion, please specify

35. Why do you think your answer to the previous question (34) is most logical?
   Please write your comments:
36. How important do you think patch management is to your organization?

☐ Not important
☐ Important only when there’s a virus/worm around the vulnerability that require patching
☐ Important only for systems/applications that are critical to business, but not all systems/applications
☐ Very important, we have an systematic way of patching out systems implemented organization-wide
☐ Very important, we only have patch management system on Windows platforms
☐ Other comments, please specify:

37. Does your IT security policy include an IT change management or configuration management policy?

☐ Yes
☐ No
☐ Not sure
☐ Not applicable, we don’t have an IT security policy

Thank you for taking the time to complete this survey.
## Appendix B: Research Log Register

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Title</th>
<th>Source File</th>
</tr>
</thead>
<tbody>
<tr>
<td>J19990806</td>
<td>1999-08-06</td>
<td>Reflection on finding of security vendor's practice of insecure programming techniques</td>
<td>J19990806.doc</td>
</tr>
<tr>
<td>J19990807</td>
<td>1999-08-07</td>
<td>Reflection and notes on finding of insecure PIN programming in Indonesian bank</td>
<td>J19990807.doc</td>
</tr>
<tr>
<td>J19990813</td>
<td>1999-08-13</td>
<td>Reflection on reset key sequence for new PDA phone and usability</td>
<td>J19990813.doc</td>
</tr>
<tr>
<td>J20000117</td>
<td>2000-01-17</td>
<td>Reflection on management decision in funding for perimeter network security project, and outsourcing of monitoring</td>
<td>J20000117.doc</td>
</tr>
<tr>
<td>J20000118</td>
<td>2000-01-18</td>
<td>Reflection on Hongkong Post Office set up of Certification Authority services and implication to the Bank</td>
<td>J20000118.doc</td>
</tr>
<tr>
<td>J20010225</td>
<td>2001-02-25</td>
<td>Reflection on inadequacies in current security practices in online Internet banking</td>
<td>J20010225.doc</td>
</tr>
<tr>
<td>J20010718</td>
<td>2001-07-18</td>
<td>Reflection on current Information Security approaches and justification for research proposal</td>
<td>J20010718.txt</td>
</tr>
<tr>
<td>J20010823</td>
<td>2001-08-23</td>
<td>Notes and reflections from learning set session with Dr Stephenie Chee focusing on Research Proposals</td>
<td>J20010823.html</td>
</tr>
<tr>
<td>J20010906</td>
<td>2001-09-06</td>
<td>Reflection on use of AR technique in a project meeting</td>
<td>J20010906.html</td>
</tr>
<tr>
<td>J20011102</td>
<td>2001-10-12</td>
<td>Reflection on current information security risk management practice in relation to social aspect of the challenges</td>
<td>J20011102.doc</td>
</tr>
<tr>
<td>J200111027</td>
<td>2001-10-27</td>
<td>Reflection and notes for Learning Set session</td>
<td>LS200111027.doc</td>
</tr>
<tr>
<td>J20020103</td>
<td>2002-01-03</td>
<td>Reflection on IRM organization, roles and responsibilities.</td>
<td>J20020103.doc</td>
</tr>
<tr>
<td>J20020205</td>
<td>2002-01-05</td>
<td>Reflection on Francis Fukuyama’s “Trust”, on the reliability of social capital and social trust in information risk management</td>
<td>J20020205.html</td>
</tr>
<tr>
<td>J20020115</td>
<td>2002-01-15</td>
<td>Notes from meetings with Line of Business stakeholders and IRMs in Hongkong</td>
<td>J20020114-15.doc</td>
</tr>
<tr>
<td>J20020118</td>
<td>2002-01-18</td>
<td>Reflection on IRM reporting and organization structure</td>
<td>J20020118.doc</td>
</tr>
<tr>
<td>J20020201</td>
<td>2002-02-01</td>
<td>Reflection on Checkland’s concept of ‘hard’ and ‘soft’ problems in the context of information risk management</td>
<td>J20020201.doc</td>
</tr>
<tr>
<td>J20020208</td>
<td>2002-02-08</td>
<td>Notes on meeting with Monetary Authority of Singapore (MAS) with regards to motivation of hackers versus systems administrators</td>
<td>J20020208.doc</td>
</tr>
<tr>
<td>J20020213</td>
<td>2002-02-13</td>
<td>Notes on Global CIRM weekly meeting, discussing status and responses to SNMP vulnerability issues</td>
<td>J20020213.txt</td>
</tr>
<tr>
<td>J20020218</td>
<td>2002-02-18</td>
<td>Reflection and notes on handling SNMP vulnerability issues with IT Services</td>
<td>J20020218.doc</td>
</tr>
<tr>
<td>J20020220</td>
<td>2002-02-20</td>
<td>Reflection and notes on meeting with Head of IT, and Business Manager in Australia subsidiary</td>
<td>J20020220.doc</td>
</tr>
</tbody>
</table>
Action Research Cycle 2 – Do Something Differently

J20020225 2002-02-25 Reflection and notes on Singapore Location Operating Committee (LOC) meeting, focusing on regulatory compliance J20020225.doc

J20020226 2002-02-26 Notes on first meeting with Regional Chief Operating Officer (COO) J20020226.doc

J20020327 2002-02-28 Reflection and notes on Japan LOC meeting J20020228.doc

J20020301 2002-03-01 Notes on meeting with regional privacy compliance officer J20020301.doc

J20020303 2002-03-03 Reflection on “Writing Well” by William Zinsser, and various information risk issues and concerns to-date J20020303.doc

J20020304 2002-03-04 Reflection and notes on meeting with Regional Head of IT Audit, focusing on roles and responsibilities of IT Audit, IRM, and IT Risk and Controls function in the region J20020304.doc

J20020305 2002-03-05 Reflection and notes on meeting with Regional IT operation manager, and regional IT manager for Investment Bank, focusing on IRM status, perception, and program J20020305.doc

J20020308 2002-03-08 Reflection and notes on meeting with Regional IT systems/infrastructure manager, focusing on role and function of IT Risk and Controls, and IRM past and present J20020308.doc

J20020311 2002-03-11 Reflection on the use of audit ratings as information risk indicators J20020311.doc

J20020312-1 2002-03-12 Reflection and Discussion notes with Managing IRM (Business Manager) on business challenges (audit & compliance) and resource lineup plan J20020312.txt

J20020312-2 2002-03-12 Reflection on the thematic concerns of information security risk management project, focusing on the primary research question J20020312-ThematicConcern.doc

J20020313-1 2002-03-13 Reflection and notes on global CIRM meeting J20020313.doc

J20020313-2 2002-03-13 Discussion notes on virus incident and updates infrastructure J20020313.txt

J20020314 2002-03-14 Feedback from Asia IRM team members J20020314.doc

J20020315 2002-03-15 Reflection and notes on meeting with Regional Head of IT, and Head of IT Townhall meeting J20020315.doc

J20020316 2002-03-16 Reflection and notes on Learning Set session J20020316.doc

J20020318 2002-03-18 Reflection on Initial Reconnaissance J20020318.doc

J20020320 2002-03-20 Reflection on dinner meeting with Japan’s Head of IT and Hongkong IRM manager on information risk management, organization culture of the Firm, and ongoing challenges faced by local staff J20020320.doc

J20020322 2002-03-22 Discussion notes on IT policy concerning use of personal PC for business J20020322.txt

J20020324 2002-03-24 Reflection on Insurance and Risk, and Discussion notes with fellow Action Researcher J20020324.txt

J20020325 2002-03-25 Plan for Global Information Risk Officer’s visit J20020325.doc

J20020326 2002-03-26 Reflection on IRM progress and status J20020326.txt

J20020327 2002-03-27 Discussion notes with team member on IRM challenges with IT Audit and business re-organization in the region J20020327.txt

J20020330 2002-03-30 Thematic analysis of CIRM and related stakeholders organizations Notes-20020330.pdf (pg 21)

J20020402 2002-04-02 Reflection on the state of IRM function as of Jan 02, 2002 J20020402.doc

J20020405 2002-04-05 Next action planning for Information Risk Management Program J20020405.doc

J20020417 2002-04-17 Discussion notes on IT Policy concerning use of J20020417.txt
<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Title</th>
<th>Source File</th>
</tr>
</thead>
<tbody>
<tr>
<td>J20020418</td>
<td>2002-04-18</td>
<td>Discussion notes and reflection on gap remediation project and issues</td>
<td>J20020418.txt</td>
</tr>
<tr>
<td>J20020430</td>
<td>2002-04-30</td>
<td>Discussion notes on IT Policy concerning customers, and inappropriate use of Risk Acceptance process; Progress in IRM Program achieving positive acknowledgement from business in Sydney</td>
<td>J20020430.txt</td>
</tr>
<tr>
<td>J20020508</td>
<td>2002-05-08</td>
<td>Reflection on communications with Regional Head of IT</td>
<td>J20020508.doc</td>
</tr>
<tr>
<td>J20020509</td>
<td>2002-05-09</td>
<td>Reflection on security status of the Firm versus global trend</td>
<td>J20020509.doc</td>
</tr>
<tr>
<td>J20020510</td>
<td>2002-05-10</td>
<td>Discussion notes on misuse of Risk Acceptance process as standard procedure for request of Generic ID, and approach to resolve issue with proper procedure established.</td>
<td>J20020510.txt</td>
</tr>
<tr>
<td>J20020527</td>
<td>2002-05-27</td>
<td>Reflection on Information Security Risk Management using Action Research Paradigm based on study result so far</td>
<td>J20020527.doc</td>
</tr>
<tr>
<td>J20020529</td>
<td>2002-05-29</td>
<td>Discussion notes with IT Services Manager reporting positive progress in IRM Program in the area of infrastructure security review. IT Services volunteering sponsorship to enhance deliverables.</td>
<td>J20020529.txt</td>
</tr>
<tr>
<td>J20020531</td>
<td>2002-05-31</td>
<td>Discussion notes with IRM in Tokyo on control issues in Business IT area, and audit preparation issues</td>
<td>J20020531.txt</td>
</tr>
<tr>
<td>J20020602</td>
<td>2002-06-02</td>
<td>Reflection on changes in organization in relation to information risk management</td>
<td>J20020602.doc</td>
</tr>
<tr>
<td>J20020607</td>
<td>2002-06-07</td>
<td>Asia IRM Offsite presentation</td>
<td>AsiaIRM-Offsite-200206078.ppt</td>
</tr>
<tr>
<td>J20020608</td>
<td>2002-06-08</td>
<td>Progress report and Reflection on progress in Learning Set session</td>
<td>J20020608.doc LS20020608.ppt</td>
</tr>
<tr>
<td>J20020609</td>
<td>2002-06-09</td>
<td>Notes on Learning Set session</td>
<td>J20020609.doc</td>
</tr>
<tr>
<td>J20020611</td>
<td>2002-06-11</td>
<td>Discussion notes on emerging SPAM problems and application security issues in business applications; Reflection on global organization challenges to staff welfare (need to stay late to keep in-sync globally)</td>
<td>J20020611.txt</td>
</tr>
<tr>
<td>J20020614</td>
<td>2002-06-14</td>
<td>Discussion notes on global IRM reporting structure and issues with global IT IRM. Gaining support from regional IT services in IRM work.</td>
<td>J20020614.txt</td>
</tr>
<tr>
<td>J20020617</td>
<td>2002-06-17</td>
<td>Discussion notes on Stakeholder Analysis with IRM; and action plans for IRM organization</td>
<td>J20020617.txt</td>
</tr>
<tr>
<td>J20020620</td>
<td>2002-06-20</td>
<td>Reflection on week of June 16, 2002</td>
<td>J20020620.txt</td>
</tr>
<tr>
<td>J20020628</td>
<td>2002-06-28</td>
<td>Discussion on Asia IRM re-organization direction and plans, including update on positive progress in current plan/activities</td>
<td>J20020628.txt</td>
</tr>
<tr>
<td>J20020628</td>
<td>2002-06-28</td>
<td>Reflection on week of June 23, 2002</td>
<td>J20020628.txt</td>
</tr>
</tbody>
</table>

**Action Research Cycle 3 – Solving the Problems**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Title</th>
<th>Source File</th>
</tr>
</thead>
<tbody>
<tr>
<td>J20020705-1</td>
<td>2002-07-05</td>
<td>Discussion on Unix remediation and infrastructure security review follow-up actions, reflecting position of IRM versus Business IT and IT Services in resource prioritization.</td>
<td>J20020705-1.txt</td>
</tr>
<tr>
<td>J20020705-2</td>
<td>2002-07-05</td>
<td>Discussion notes on with IRM member on IRM regular communication report to external stakeholders and issues in IRM organization/resources</td>
<td>J20020705-2.txt</td>
</tr>
<tr>
<td>J20020705-3</td>
<td>2002-07-05</td>
<td>Discussion notes with Sydney IRM member on IRM re-organization structure and deliberated on roles of IRM security services team and assignment</td>
<td>J20020705-3.txt</td>
</tr>
<tr>
<td>J20020710-1</td>
<td>2002-07-10</td>
<td>Discussion notes on IRM resources, and more</td>
<td>J20020710-1.txt</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>J20020710-2</td>
<td>2002-07-10</td>
<td>Discussion notes on security advisory communication and mailing list issue raised by IT Services</td>
<td>J20020710-2.txt</td>
</tr>
<tr>
<td>J20020712-1</td>
<td>2002-07-12</td>
<td>Discussion on closure to security advisory issue; patch deployment process; and IRM review report structure and distribution</td>
<td>J20020712.txt</td>
</tr>
<tr>
<td>J20020712-2</td>
<td>2002-07-12</td>
<td>Reflection on the fundamentals of information risk management and how they relate to the practice and the Firm</td>
<td>J20020712.doc</td>
</tr>
<tr>
<td>J20020715</td>
<td>2002-07-15</td>
<td>Notes on action plan for Global Head of IRM visit to region</td>
<td>J20020715.doc</td>
</tr>
<tr>
<td>J20020717</td>
<td>2002-07-17</td>
<td>Reflection and notes on risk assessment of Korean business information risk</td>
<td>J20020717-17.doc</td>
</tr>
<tr>
<td>J20020719</td>
<td>2002-07-19</td>
<td>Reflection and notes on meeting with Head of Equities business application development team in Japan – issues of IRM roles, functions, organizations, and reporting remained a concern to the business</td>
<td>J20020719.doc</td>
</tr>
<tr>
<td>J20020722</td>
<td>2002-07-22</td>
<td>Discussion notes on security workflow and responsibilities between IT services (security administration) and IRM role in the process</td>
<td>J20020722.txt</td>
</tr>
<tr>
<td>J20020723</td>
<td>2002-07-23</td>
<td>Reflection and notes on Japan LOC meeting and positive outcome achieved</td>
<td>J20020723.doc</td>
</tr>
<tr>
<td>J20020729-1</td>
<td>2002-07-29</td>
<td>Notes and reflection on first meeting with Regional Chief Operating Officer (COO), as new business report for IRM team</td>
<td>J20020729.txt</td>
</tr>
<tr>
<td>J20020729-2</td>
<td>2002-07-29</td>
<td>Notes and reflection on meeting with Global Head of IRM</td>
<td>J20020729.doc</td>
</tr>
<tr>
<td>J20020730</td>
<td>2002-07-30</td>
<td>Reflection and notes from Media Training by ITSC (for role as Chairman of IT Security Standards Committee) – on perception of public and the role of the media</td>
<td>J20020730.doc</td>
</tr>
<tr>
<td>J20020806</td>
<td>2002-08-06</td>
<td>Discussion notes with IRM member on IT Audit’s role in IRM program; and progress of IRM activities in the region.</td>
<td>J20020806.txt</td>
</tr>
<tr>
<td>J20020812</td>
<td>2002-08-12</td>
<td>Reflection on reading of “India Unbound” and the design of information security risk management approach/model</td>
<td>J20020812.doc</td>
</tr>
<tr>
<td>J20020813</td>
<td>2002-08-13</td>
<td>Reflection and notes on meeting with Regional Head of IT, focusing on IRM status and IT/Business perception</td>
<td>J20020813.doc</td>
</tr>
<tr>
<td>J20020815</td>
<td>2002-08-15</td>
<td>Reflection and discussion note with IRM member following regional senior management meeting on security issues in business application administration areas</td>
<td>J20020815.txt</td>
</tr>
<tr>
<td>J20020817</td>
<td>2002-08-17</td>
<td>Reflection on week of Aug 12, 2002</td>
<td>J20020817.doc</td>
</tr>
<tr>
<td>J20020819</td>
<td>2002-08-19</td>
<td>Discussion with IRM member and reflection on status of IRM program and organizational issues</td>
<td>J20020819.txt</td>
</tr>
<tr>
<td>J20020821</td>
<td>2002-08-21</td>
<td>Reflection and notes on meeting with business, IT, and IRM in India subsidiary</td>
<td>J20020821.doc</td>
</tr>
<tr>
<td>J20020824-1</td>
<td>2002-08-24</td>
<td>Reflection on quantitative risk assessment methodology</td>
<td>J20020824.doc</td>
</tr>
<tr>
<td>J20020824-2</td>
<td>2002-08-24</td>
<td>Reflection and discussion note on Learning Set session</td>
<td>LS20020824.ppt</td>
</tr>
<tr>
<td>J20020826</td>
<td>2002-08-26</td>
<td>Reflection on concept of Supply and Demand in relation to IRM function</td>
<td>J20020826.doc</td>
</tr>
<tr>
<td>J20020826-2</td>
<td>2002-08-26</td>
<td>Notes on Top five IT security issues</td>
<td>J20020826-2.doc</td>
</tr>
<tr>
<td>J20020826-3</td>
<td>2002-08-26</td>
<td>Notes on commonly asked questions about IRM function</td>
<td>J20020826-3.doc</td>
</tr>
<tr>
<td>J20020907-1</td>
<td>2002-09-07</td>
<td>Reflection on “Zen and the Art of Motorcycle”</td>
<td>J20020907.doc</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>J20020907-2</td>
<td>2002-09-07</td>
<td>Maintenance” triggering the idea of storytelling for information risk awareness</td>
<td>J20020907-20020907-Octave.doc</td>
</tr>
<tr>
<td>J20020908</td>
<td>2002-09-08</td>
<td>Reflection on reading of book on OCTAVE risk assessment methodology</td>
<td>J20020908.txt</td>
</tr>
<tr>
<td>J20020909-1</td>
<td>2002-09-09</td>
<td>Notes on email discussion with fellow Action Researcher on research issues</td>
<td>J20020909-1.txt</td>
</tr>
<tr>
<td>J20020909-2</td>
<td>2002-09-09</td>
<td>Reflection on Investment Bank's inaugural Technology Control Council meeting</td>
<td>J20020909.doc</td>
</tr>
<tr>
<td>J20020910-1</td>
<td>2002-09-10</td>
<td>Reflection and notes of learning set session with fellow Action Researcher – the concept of 'D-day' preparation, which led to use of Piezoelectric material as a metaphor emerged from this meeting</td>
<td>J20020910.doc</td>
</tr>
<tr>
<td>J20020911-3</td>
<td>2002-09-13</td>
<td>Reflection on week of Sep 9, 2002</td>
<td>J20020913.doc</td>
</tr>
<tr>
<td>J20020914-1</td>
<td>2002-09-14</td>
<td>Reflection on issue of perception management as brought up by Regional Head of IT Services</td>
<td>Notes-20020901.pdf (pg 29); transcribed in J20020914.txt</td>
</tr>
<tr>
<td>J20020914-2</td>
<td>2002-09-14</td>
<td>Reflection on meeting with Investment Bank's application development team, and discussion session with Boon-Hou (2002-09-09) on status of IRM in the Firm</td>
<td>J20020914.doc</td>
</tr>
<tr>
<td>J20020920</td>
<td>2002-09-20</td>
<td>Reflecting on Information Security Risk Assessment (ISRA) methodology used in the Firm and implication to the research</td>
<td>J20020920.txt</td>
</tr>
<tr>
<td>J20020921</td>
<td>2002-09-21</td>
<td>Reflection on week of Sep 16, 2002</td>
<td>J20020921.doc</td>
</tr>
<tr>
<td>J20020925</td>
<td>2002-09-25</td>
<td>Reflection on IRM approach – Policy compliance versus risk-based</td>
<td>Notes-20020901-pdf (pg 45-47)</td>
</tr>
<tr>
<td>J20021005</td>
<td>2002-10-05</td>
<td>Notes on feedback from Line of Business in Japan, and Business Head's volunteer translation of IRM training material to business-friendly language</td>
<td>J20021005.doc</td>
</tr>
<tr>
<td>J20021012-1</td>
<td>2002-10-12</td>
<td>Reflection and notes on regional IT and Equities' application security issues</td>
<td>J20021012.txt</td>
</tr>
<tr>
<td>J20021018-1</td>
<td>2002-10-18</td>
<td>Reflection and notes on meeting with external auditor and discussion on IRM function, roles, and responsibilities, and current practices</td>
<td>J20021018.doc</td>
</tr>
<tr>
<td>J20021018-2</td>
<td>2002-10-18</td>
<td>Reflection and notes on key information security and risk issues in the region</td>
<td>J20021018.txt</td>
</tr>
<tr>
<td>J20021001</td>
<td>2002-11-01</td>
<td>Reflection on security awareness program</td>
<td>Notes-20021001.pdf (pg 52)</td>
</tr>
<tr>
<td>J20021002</td>
<td>2002-11-02</td>
<td>Notes on Risk Profile and Global Head of IRM's view of the function/role of IRM</td>
<td>Notes-20021001.pdf (pg 54-55)</td>
</tr>
<tr>
<td>J20021107</td>
<td>2002-11-07</td>
<td>Reflection and notes on current practices triggered from lunch discussion with former colleagues in government department</td>
<td>J20021107.txt</td>
</tr>
<tr>
<td>J20021108-1</td>
<td>2002-11-08</td>
<td>Discussion notes with fellow Action Researcher on progress status, issues/dilemmas, and action strategies</td>
<td>J20021108.pdf</td>
</tr>
<tr>
<td>J20021108-2</td>
<td>2002-11-08</td>
<td>Discussion notes with Regional Head of IT Services on outsourcing project. Use of scenarios was suggested to identify roles of IRM in outsourcing transition</td>
<td>Notes-20021101-1231.pdf (pg 12)</td>
</tr>
<tr>
<td>J20021113</td>
<td>2002-11-13</td>
<td>Discussion notes with IRM member on time-based security, and the consideration of time factor and information flow in risk assessment, introducing time as a graph with values between 0 and 1.</td>
<td>J20021113.txt</td>
</tr>
<tr>
<td>J20021108</td>
<td>2002-11-16</td>
<td>Notes and reflection from learning set session with</td>
<td>J20021108.pdf</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>J20021127</td>
<td>2002-11-27</td>
<td>Discussion notes with global IRM on pros and cons of global IRM re-organization and reporting plan/directions</td>
<td>J20021127.txt</td>
</tr>
<tr>
<td>J20021205-1</td>
<td>2002-12-05</td>
<td>Reflection and notes on Chinese Wall/Firewall Policies and regulatory compliance in Japan</td>
<td>Notes-20021118-1205.pdf (pg 31-34)</td>
</tr>
<tr>
<td>J20021205-2</td>
<td>2002-12-05</td>
<td>Reflection and notes on IRM organizations – globally, regionally, and locally to provide effective location and business supports</td>
<td>Notes-20021118-1205.pdf (pg 1-30)</td>
</tr>
<tr>
<td>J20021206</td>
<td>2002-12-06</td>
<td>What are the motivating factors for IRM to do better?</td>
<td>J20021206.txt</td>
</tr>
<tr>
<td>J20021209</td>
<td>2002-12-09</td>
<td>Reflection on Time-based Security approach                                                                iline</td>
<td>J20021209.doc</td>
</tr>
<tr>
<td>J20021217</td>
<td>2002-12-17</td>
<td>Discussion notes with global IRM on global proposed new IRM operating model</td>
<td>J20021217.txt</td>
</tr>
<tr>
<td>J20021219</td>
<td>2002-12-24</td>
<td>Reflection on week of Dec 19, 2002</td>
<td>J20021219.doc</td>
</tr>
<tr>
<td>J20021230-1</td>
<td>2002-12-30</td>
<td>Reflection and notes on research status and current issues (with email discussion with fellow Action Researcher)</td>
<td>J20021230.txt</td>
</tr>
<tr>
<td>J20021230-2</td>
<td>2003-01-02</td>
<td>Reflection and notes on Asia IRM team meeting</td>
<td>Notes-20030102-02.pdf (pg 1-2)</td>
</tr>
<tr>
<td>J20021230-3</td>
<td>2003-01-08</td>
<td>Reflection and notes on meeting with Asset Management's Business IT functional head</td>
<td>Notes-20030102-03.pdf (pg 12)</td>
</tr>
<tr>
<td>J20030109-1</td>
<td>2003-01-09</td>
<td>Reflection and notes on meeting with Regional Head of IT Services</td>
<td>J20030109.rtf</td>
</tr>
<tr>
<td>J20030109-2</td>
<td>2003-01-09</td>
<td>Reflection and notes on Chinese Wall/Firewall policy compliance in Japan</td>
<td>Notes-20030102-03.pdf (pg 16-17)</td>
</tr>
<tr>
<td>J20030110</td>
<td>2003-01-10</td>
<td>Reflection and notes on new IRM organization (or rather, re-organization) to decentralize IRM to individual Line of Business</td>
<td>J20030110.rtf</td>
</tr>
<tr>
<td>J20030120-1</td>
<td>2003-01-20</td>
<td>Discussion notes with global IRM on transition for IRM member to new operating model</td>
<td>J20030120.txt</td>
</tr>
<tr>
<td>J20030120-3</td>
<td>2003-01-20</td>
<td>Assessment of CIRM-Asia using SSM CATWOE approach</td>
<td>J20030120-CATWOE.doc</td>
</tr>
<tr>
<td>J20020123</td>
<td>2003-01-23</td>
<td>Discussion notes on role of IRM in assurance of IT policy implementation</td>
<td>J20020123.txt</td>
</tr>
<tr>
<td>J20030124</td>
<td>2003-01-24</td>
<td>Notes on Piezoelectric risk management approach</td>
<td>J20030124.txt</td>
</tr>
<tr>
<td>J20030125-1</td>
<td>2003-01-25</td>
<td>Initial thoughts and discussion with fellow Action Researcher on thesis report structure</td>
<td>J20030125.txt</td>
</tr>
<tr>
<td>J20030125-2</td>
<td>2003-01-25</td>
<td>Reflection and discussion notes for Learning Set session</td>
<td>LS20030125.ppt</td>
</tr>
<tr>
<td>J20030127</td>
<td>2003-01-27</td>
<td>Discussion notes on generic ID request/issuance process with Japan Head of IT Services</td>
<td>J20030127.txt</td>
</tr>
<tr>
<td>J20030128</td>
<td>2003-01-28</td>
<td>Notes on Japan FSA comments on inadequate IRM resources in Tokyo to support business needs</td>
<td>J20030128.txt</td>
</tr>
<tr>
<td>J20030129</td>
<td>2003-01-29</td>
<td>Discussion notes with LOB IRM on audit issues remediation in LOB, and related IRM responsibility</td>
<td>J20030129.txt</td>
</tr>
<tr>
<td>J20030201</td>
<td>2003-02-01</td>
<td>Reflection on security policies</td>
<td>J20030201.doc</td>
</tr>
<tr>
<td>J20030209</td>
<td>2003-02-09</td>
<td>Reflection on current findings with draft presentation proposal reconsidering IT security, business continuity, and disaster recovering planning practices</td>
<td>J20030209.ppt</td>
</tr>
<tr>
<td>J20030212</td>
<td>2003-02-12</td>
<td>Discussion notes with Line of Business IRM on 2003 application security review plan – issue of not catering for changes in business highlighted</td>
<td>J20030212.txt</td>
</tr>
<tr>
<td>J20030305</td>
<td>2003-03-05</td>
<td>Discussion notes on regulatory requirements and compliance readiness for IT outsourcing in the region</td>
<td>Notes-20031002-02.pdf (pg 13-14)</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>J20030310</td>
<td>2003-03-10</td>
<td>Reflection and notes on Global Information Risk Officer's visit and meetings with regional key stakeholders</td>
<td>Notes-200310-0321.pdf</td>
</tr>
<tr>
<td>J20030313</td>
<td>2003-03-13</td>
<td>Reflection and notes on meeting with regional compliance covering ID Re-certification issues, Awareness training, Information Owner, and roles/responsibilities issues</td>
<td>Notes-200310-0321.pdf (pg 7-8)</td>
</tr>
<tr>
<td>J20030317</td>
<td>2003-03-17</td>
<td>Discussion notes with Business Operations on issues relating to Information Owner Policy and practices</td>
<td>Notes-200310-0321.pdf (pg 14)</td>
</tr>
<tr>
<td>J20030318</td>
<td>2003-03-18</td>
<td>Reflection on &quot;need to have more teeth&quot; to get things done with sustainability and integrity</td>
<td>Notes-200310-0321.pdf (pg 15)</td>
</tr>
<tr>
<td>J20030320</td>
<td>2003-03-20</td>
<td>Discussion notes on OCTAVE methodology, and information security versus information risk functions</td>
<td>Notes-200310-0321.pdf (pg 18-20)</td>
</tr>
<tr>
<td>J20030401-1</td>
<td>2003-04-01</td>
<td>Reflection on data analysis and first discourse on theme of &quot;criticality effect&quot;</td>
<td>J20030401-Criticality.doc</td>
</tr>
<tr>
<td>J20030401-2</td>
<td>2003-04-01</td>
<td>Managing information risk in the event of a SARS Outbreak – notes and reflection</td>
<td>J20030401-SARS.doc</td>
</tr>
<tr>
<td>J20030402</td>
<td>2003-04-02</td>
<td>Discussion notes with IRM on managing information risk in SARS contingency – infrastructure not ready to support needs of situation</td>
<td>J20030402.txt</td>
</tr>
<tr>
<td>J20030407-1</td>
<td>2003-04-07</td>
<td>Collections of notes taken in March 2003 – understanding on patch issues</td>
<td>Notes-200303.pdf</td>
</tr>
<tr>
<td>J20030407-2</td>
<td>2004-04-07</td>
<td>Collections of notes taken during discussions from April to 15 May 2003 – includes thoughts on scenario planning, interview questioning, organization structure, risk metrics, SARS incident, gap remediation, IRM Program, ID Admin issues, and Asia IRM meeting.</td>
<td>Notes-200304-05-1.pdf</td>
</tr>
<tr>
<td>J20030410</td>
<td>2003-04-10</td>
<td>Creation of gap remediation scorecard according to new global template</td>
<td>J20030410.pdf</td>
</tr>
<tr>
<td>J20030403</td>
<td>2003-04-03</td>
<td>Use of home PC with company software in view of SARS contingency (1)</td>
<td>J20030403.pdf</td>
</tr>
<tr>
<td>J20030407-3</td>
<td>2003-04-07</td>
<td>Use of home PC with company software in view of SARS contingency (2)</td>
<td>J20030407-3.pdf</td>
</tr>
<tr>
<td>J20030407-4</td>
<td>2003-04-07</td>
<td>Discussion notes on new IRM structure and how to address specific location issues and requirements with IRM member</td>
<td>J20030407-4.pdf</td>
</tr>
<tr>
<td>J20030409-1</td>
<td>2003-04-09</td>
<td>Notes and reflection from weekly Asia IRM meeting</td>
<td>J20030409-1.pdf</td>
</tr>
<tr>
<td>J20030409-2</td>
<td>2003-04-09</td>
<td>Discussion notes (with IRM) on Bank of Negara online banking security requirements and responses</td>
<td>J20030409-2.pdf</td>
</tr>
<tr>
<td>J20030411</td>
<td>2003-04-11</td>
<td>Discussion notes with IRM on IRM re-alignment and changes in business structure</td>
<td>J20030411.pdf</td>
</tr>
<tr>
<td>J20030412</td>
<td>2003-04-12</td>
<td>Use of home PC with company software in view of SARS contingency (3)</td>
<td>J20030412.pdf</td>
</tr>
<tr>
<td>J20030413</td>
<td>2003-04-13</td>
<td>Reflection on IT paper highlighting reliance on technology to solve security issues</td>
<td>NotesCard mdi</td>
</tr>
<tr>
<td>J20030414</td>
<td>2003-04-14</td>
<td>Reflection on business bureaucracies and Model 1 Learning</td>
<td>NotesCard mdi</td>
</tr>
<tr>
<td>J20030416</td>
<td>2003-04-16</td>
<td>Reflection on Donald Schon’s “Reflective Practitioners” conclusion chapter in relation to IRM practice and issues</td>
<td>NotesCard mdi</td>
</tr>
<tr>
<td>J20030413</td>
<td>2003-04-21</td>
<td>Discussion notes on topics for IRM Learning Group sessions</td>
<td>J20030413.pdf</td>
</tr>
<tr>
<td>J20030422-1</td>
<td>2003-04-22</td>
<td>Reflection and discussion notes with IRM on decentralized IRM organization model</td>
<td>J20030422.doc</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>J20030422-2</td>
<td>2003-04-22</td>
<td>Discussion notes and reflection on infrastructure readiness for SARS contingency and needs to focus on such critical incident in IRM program</td>
<td>J20030422-1.txt</td>
</tr>
<tr>
<td>J20030422-3</td>
<td>2003-04-22</td>
<td>Discussion notes on IRM re-alignment for new operating model, and reflection on SARS contingency problem and SQL Slammer incident security readiness</td>
<td>J20030422-2.txt</td>
</tr>
<tr>
<td>J20030423</td>
<td>2003-04-23</td>
<td>Reflection and notes on meeting with Japan Head of IT and HR department with regards to implementation of decentralization IRM organization model</td>
<td>J20030423.doc</td>
</tr>
<tr>
<td>J20030425</td>
<td>2003-04-25</td>
<td>Reflection on Donald Schon’s “Reflective Practitioners” in relation to IRM practices and competency</td>
<td>J20030425.doc</td>
</tr>
<tr>
<td>J20030426</td>
<td>2003-04-26</td>
<td>Reflection and notes for Learning Set session focusing on thesis framework</td>
<td>LS20030426.ppt</td>
</tr>
<tr>
<td>J20030429</td>
<td>2003-04-29</td>
<td>Reflection and Discussion notes of information security management standards and practices with ISO security standards expert</td>
<td>J20030429.doc</td>
</tr>
<tr>
<td>J20030503-1</td>
<td>2003-05-03</td>
<td>Reflection on Garner’s article on managing risk</td>
<td>NotesCard.mdi</td>
</tr>
<tr>
<td>J20030503-2</td>
<td>2003-05-03</td>
<td>Reflection on AREOL Session 10 in relation to empowerment of IRM</td>
<td>NotesCard.mdi</td>
</tr>
<tr>
<td>J20030504</td>
<td>2003-05-04</td>
<td>Notes from reading of Dalai Lama's book on Happiness (relevance to security training)</td>
<td>NotesCard.mdi</td>
</tr>
<tr>
<td>J20030509</td>
<td>2003-05-09</td>
<td>Reflection on current approach and issues in motivating effective information risk management practices</td>
<td>NotesCard.mdi</td>
</tr>
<tr>
<td>J20030510</td>
<td>2003-05-10</td>
<td>Updated thesis framework incorporating ideas from latest reflections</td>
<td>LS20030510.ppt</td>
</tr>
<tr>
<td>J20030511</td>
<td>2003-05-11</td>
<td>Reflection and notes on “Threshold of Criticality”</td>
<td>NotesCard.mdi</td>
</tr>
<tr>
<td>J20030513</td>
<td>2003-05-13</td>
<td>Discussion notes with global IRM on IRM re-organization issues and challenges</td>
<td>J20030513.txt</td>
</tr>
<tr>
<td>J20030523</td>
<td>2003-05-23</td>
<td>Reflection and notes on the notion of Fear, Uncertainty and Doubt (FUD), and the principle of “Criticality Effect”</td>
<td>NotesCard.mdi</td>
</tr>
<tr>
<td>J20030524</td>
<td>2003-05-24</td>
<td>Reflection on IRM and management use of security information</td>
<td>J20030524.doc</td>
</tr>
<tr>
<td>J20030526-1</td>
<td>2003-05-26</td>
<td>Notes and reflection on the cost of policy compliance (resulting from Enron case affecting the Firm.)</td>
<td>J20030526-CostOfPolicy.txt</td>
</tr>
<tr>
<td>J20030526-2</td>
<td>2003-05-26</td>
<td>Notes on discourses with fellow practitioner on evolving information security risk management approach, focusing on reaction and compartmentalization</td>
<td>J20030526.doc</td>
</tr>
<tr>
<td>J20030529</td>
<td>2003-05-29</td>
<td>Reflection and notes on Information Security Forum (ISF) regional risk analysis methodology workshop</td>
<td>J20030529.doc</td>
</tr>
<tr>
<td>J20030531</td>
<td>2003-05-31</td>
<td>Reflection and notes on Learning Set session</td>
<td>J20030531.doc LS20030531.ppt</td>
</tr>
<tr>
<td>J20030604-1</td>
<td>2003-06-04</td>
<td>Discussion with IT Auditor on Controls versus Risk, and Awareness versus Actionable Knowledge</td>
<td>J20030604.txt</td>
</tr>
<tr>
<td>J20030503-3</td>
<td>2003-06-04</td>
<td>Reflection on series of IRM and IT Auditors’ discussions on Controls versus Risk</td>
<td>J20030604.doc</td>
</tr>
<tr>
<td>J20030605</td>
<td>2003-06-05</td>
<td>Discussion notes capturing the closure of resource alignment for new IRM structure in the region</td>
<td>J20030605.txt</td>
</tr>
<tr>
<td>J20030607</td>
<td>2003-06-07</td>
<td>Reflection on the idea of “criticality effect” in reducing redundancy in IRM practices</td>
<td>J20030607.doc</td>
</tr>
<tr>
<td>J20030610</td>
<td>2003-06-10</td>
<td>Reflection and notes on ID Admin function and practices</td>
<td>J20030610.doc</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>J20030612-1</td>
<td>2003-06-12</td>
<td>Reflection and Discussion notes with IRM members on IRM alignment with Line of Business (decentralization of IRM organization)</td>
<td>J20030612.doc</td>
</tr>
<tr>
<td>J20030612-2</td>
<td>2003-06-12</td>
<td>Discussion notes with IRM member capturing reflection on Control Self Assessment (CSA) inadequacies, and potential problem in IRM being part of the business</td>
<td>J20030612.txt</td>
</tr>
<tr>
<td>J20030627-1</td>
<td>2003-06-27</td>
<td>Discussion notes with IRM member on Control versus Risk, and idea of using customer value as a risk value indicator</td>
<td>J20030627.txt</td>
</tr>
<tr>
<td>J20030629-1</td>
<td>2003-06-29</td>
<td>Reflection and notes on meeting with business on banking secrecy issues and action plan</td>
<td>J20030629.doc</td>
</tr>
<tr>
<td>J20030629-2</td>
<td>2003-06-29</td>
<td>Reflection and notes on Learning Set session capturing reflection on Control Self Assessment inadequacies, and potential problem in IRM being part of the business</td>
<td>J20030629.txt</td>
</tr>
<tr>
<td>J20030705</td>
<td>2003-07-05</td>
<td>Reflection on reading Peter Dennings' articles on &quot;Career Redux&quot; and &quot;Accomplishment – Language-action philosophy uncovers the truth about effective coordination and accomplishment&quot; in relation to IRM practices</td>
<td>J20030705.doc</td>
</tr>
<tr>
<td>J20030708</td>
<td>2003-07-08</td>
<td>Reflecting on current practice and mapping aspects of information security in pictorial form for evaluation</td>
<td>J20030708.ppt</td>
</tr>
<tr>
<td>J20030711</td>
<td>2003-07-11</td>
<td>Issues in IRM practice (documentation and sharing of interim solutions)</td>
<td>J20030711.txt</td>
</tr>
<tr>
<td>J20030818</td>
<td>2003-08-18</td>
<td>Reflection on SQL Slammer and Blaster incidents in the Firm</td>
<td>J20030818.doc</td>
</tr>
<tr>
<td>J20030919</td>
<td>2003-09-19</td>
<td>Reflection on IRM Practices and opportunities for improvements</td>
<td>J20030919.doc</td>
</tr>
<tr>
<td>Action Research Cycle 5 – Understanding Responsiveness</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>J20031115</td>
<td>2003-11-15</td>
<td>Reflection and notes for Learning Set session</td>
<td>LS20031115.ppt</td>
</tr>
<tr>
<td>J20031118</td>
<td>2003-11-18</td>
<td>Presentation to HK Information Security Summit on &quot;Observations and Thoughts on Information Risk Management&quot;</td>
<td>J20031118.ppt</td>
</tr>
<tr>
<td>J20040226</td>
<td>2004-02-26</td>
<td>Reflection and notes on panel discussion in IDC security conference</td>
<td>J20040226.doc</td>
</tr>
<tr>
<td>J20040301</td>
<td>2004-03-01</td>
<td>Planning notes on identifying APAC local security requirements</td>
<td>J20040301.doc</td>
</tr>
<tr>
<td>J20040431</td>
<td>2004-04-31</td>
<td>Analysis of Sasser worm propagation techniques</td>
<td>J20040431.ppt</td>
</tr>
<tr>
<td>J20040510</td>
<td>2004-05-10</td>
<td>Reflection on discussions with BETA staff involved in Blaster and SQL Slammer incidents, triggered from findings in Sasser worm incident</td>
<td>J20040510.doc</td>
</tr>
<tr>
<td>J20040608</td>
<td>2004-06-08</td>
<td>Reflection on responsive security strategy on reading Sun Tze's Art of War</td>
<td>OneNote20040608</td>
</tr>
<tr>
<td>J20040701</td>
<td>2004-07-01</td>
<td>Reflection and notes for Learning Set session, including reflection on Australia Cybercrime Conference follow-up meeting in June 2004</td>
<td>LS20040701.ppt</td>
</tr>
<tr>
<td>J20040702</td>
<td>2004-07-02</td>
<td>Reflection on discussion with Bob Dick on Responsive security strategy (in Brisbane)</td>
<td>OneNote20040702</td>
</tr>
<tr>
<td>J20040712</td>
<td>2004-07-12</td>
<td>Reflection on reading &quot;Myths of Homeland Security&quot; by Marcus Ranum</td>
<td>J20040712.doc</td>
</tr>
<tr>
<td>J20040718</td>
<td>2004-07-18</td>
<td>Reflection and notes on Responsive Security Strategy</td>
<td>OneNote20040718</td>
</tr>
<tr>
<td>J20040719</td>
<td>2004-07-19</td>
<td>Reflection and notes on Responsive Security Strategy</td>
<td>J20040719.doc</td>
</tr>
<tr>
<td>J20040830</td>
<td>2004-08-30</td>
<td>Reflection on Customer Relationship Management (CRM) system and its relation to implementing security (changing mindset)</td>
<td>OneNote20040830</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>J20040908</td>
<td>2004-09-08</td>
<td>Reflection on comparison of business impact assessment in business continuity planning and information security risk assessment</td>
<td>OneNote20040908</td>
</tr>
<tr>
<td>J20040925</td>
<td>2004-09-25</td>
<td>Reflection on security communications</td>
<td>OneNote20040925</td>
</tr>
<tr>
<td>J20040926</td>
<td>2004-09-26</td>
<td>Reflection on human immune system and its relation to information security risk management</td>
<td>OneNote20040926</td>
</tr>
<tr>
<td>J20041010</td>
<td>2004-10-10</td>
<td>Reflection on thesis writing</td>
<td>J20041010.doc</td>
</tr>
<tr>
<td>J20041015</td>
<td>2004-10-15</td>
<td>Reflection and notes on Game Theory and implications to information security risk management</td>
<td>OneNote20041015.doc</td>
</tr>
<tr>
<td>J20041024</td>
<td>2004-10-24</td>
<td>Reflection on motivation for security vendors to solve security problems – fundamental contradiction of objectives</td>
<td>OneNote20041024</td>
</tr>
<tr>
<td>J20041026</td>
<td>2004-10-26</td>
<td>Reflection and notes on Literature Review chapter for thesis report</td>
<td>J20041026.doc</td>
</tr>
<tr>
<td>J20041027</td>
<td>2004-10-27</td>
<td>Reflection on how information risk are being managed in customers' enterprises</td>
<td>OneNote20041027</td>
</tr>
<tr>
<td>J20041104</td>
<td>2004-11-04</td>
<td>Reflection on E-Readiness Indicator used in UN-ECAP versus idea of Responsive Index</td>
<td>OneNote20041104</td>
</tr>
<tr>
<td>J20041112</td>
<td>2004-11-12</td>
<td>Reflection on reading “Predictable Surprises”</td>
<td>J20041112.doc</td>
</tr>
<tr>
<td>J20041204</td>
<td>2004-12-04</td>
<td>Reflection on responsiveness – triggered by rain in Disneyland, California</td>
<td>J20041204.doc</td>
</tr>
<tr>
<td>J20041225</td>
<td>2004-12-25</td>
<td>Reflection and solution brainstorming on responsive security strategy</td>
<td>OneNote20041225</td>
</tr>
<tr>
<td>J20041226-1</td>
<td>2004-12-26</td>
<td>Reflection on Tsunami incident in Asia</td>
<td>J20041226.doc</td>
</tr>
<tr>
<td>J20041226-2</td>
<td>2004-12-26</td>
<td>Discussion notes on Case Study versus Evaluation</td>
<td>OneNote20041226</td>
</tr>
<tr>
<td>J20041227-1</td>
<td>2004-12-27</td>
<td>Reflection on current practices in information security risk management (observation of other organizations' practices)</td>
<td>J20041227.doc</td>
</tr>
<tr>
<td>J20041227-2</td>
<td>2004-12-27</td>
<td>Reflection and notes of learning set session with fellow Action Researcher on research issues, status, and thesis writing</td>
<td>J20041227-BHarmend.doc</td>
</tr>
<tr>
<td>J20041229</td>
<td>2004-12-29</td>
<td>Reflection and notes on meeting with Organization ALPHA's IRM members</td>
<td>J20041229.doc</td>
</tr>
<tr>
<td>J20041231</td>
<td>2004-12-31</td>
<td>Reflection and additional notes on meeting with fellow Action Researcher on Dec 27, 2004</td>
<td>J20041231.doc</td>
</tr>
<tr>
<td>J20050110</td>
<td>2005-01-10</td>
<td>Reflection on discussion with Information Security Professionals on current practices and challenges (at IS2C Asia Advisory Board meeting)</td>
<td>J20050110.doc</td>
</tr>
<tr>
<td>J20050112</td>
<td>2005-01-12</td>
<td>Reflection and Discussion notes with external audit partner on current IT compliance regime and challenges</td>
<td>J20050112.doc</td>
</tr>
<tr>
<td>J20050113</td>
<td>2005-01-13</td>
<td>Reflection and Discussion notes with external audit partner on IT security issues and practices</td>
<td>J20050113(2).doc</td>
</tr>
<tr>
<td>J20050123</td>
<td>2005-01-23</td>
<td>Reflection and notes from various readings relating to IT security and action research methodologies</td>
<td>J20050123.doc</td>
</tr>
<tr>
<td>J20050319</td>
<td>2005-03-19</td>
<td>Reflection, notes and progress report in Learning Set session</td>
<td>LS20050319.ppt OneNote20050319</td>
</tr>
<tr>
<td>J20050327</td>
<td>2005-03-27</td>
<td>Reflection and discussion notes on thesis organization, structure, and writing (with fellow Action Researcher)</td>
<td>OneNote20050327</td>
</tr>
<tr>
<td>J20050630-1</td>
<td>2005-06-30</td>
<td>Reflection on IT outsourcing revisited</td>
<td>OneNote20050630-1</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>J20050630-2</td>
<td>2005-06-30</td>
<td>Notes and reflection on FIRST Corporate Executive Program (CEP) workshop</td>
<td>OneNote20050630</td>
</tr>
<tr>
<td>J20050630-3</td>
<td>2005-06-30</td>
<td>Reflection on issues relating to approaches based on “weakest link” principle</td>
<td>OneNote20050630-2</td>
</tr>
<tr>
<td>J20050711</td>
<td>2005-07-11</td>
<td>Reflection and notes on series of meetings with Organization CHARLIE on security challenges and possible use of responsive security approach and related framework</td>
<td>J20050711.doc</td>
</tr>
<tr>
<td>J20050712</td>
<td>2005-07-12</td>
<td>Reflection and notes on research findings and preliminary conclusions</td>
<td>LS20050712.ppt</td>
</tr>
<tr>
<td>J20050715</td>
<td>2005-07-15</td>
<td>Reflection and notes on research findings and revised preliminary conclusions</td>
<td>LS20050715.ppt</td>
</tr>
<tr>
<td>J20050731</td>
<td>2005-07-31</td>
<td>Reflection on analytical philosophy and its possible interpretation from an information security risk management perspective</td>
<td>OneNote20050731</td>
</tr>
<tr>
<td>J20050826</td>
<td>2005-08-26</td>
<td>Reflection and discussion notes (with fellow Action Researcher) on justifying responsive security using Strawson’s analytical philosophy</td>
<td>OneNote20050826</td>
</tr>
<tr>
<td>J20050827</td>
<td>2005-08-27</td>
<td>Reflection and discussion notes (with fellow Action Researcher) on risk management planning</td>
<td>OneNote20050827</td>
</tr>
<tr>
<td>J20050902</td>
<td>2005-09-02</td>
<td>Reflection and notes on Responsive Security approach and thinking on privacy challenges that are of concerns to government now</td>
<td>J20050902.doc</td>
</tr>
<tr>
<td>J20050905</td>
<td>2005-09-05</td>
<td>Notes on OECD Security Guidelines including responsibility and response the top three principles for implementing a “culture of security”</td>
<td>OneNote20050905</td>
</tr>
<tr>
<td>J20050911</td>
<td>2005-09-11</td>
<td>Reflection and discussion notes (with fellow Action Researcher) on Scenario Based Training (SBT)</td>
<td>OneNote20050911</td>
</tr>
<tr>
<td>J20050912</td>
<td>2005-09-12</td>
<td>Reflection from second reading of Checkland’s SSM series</td>
<td>J20050912-Checkland.doc</td>
</tr>
<tr>
<td>J20050913</td>
<td>2005-09-13</td>
<td>Reflection on presentation on Responsive Security approach in ManilaCon conference in Manila, the Philippines</td>
<td>J20050913.doc</td>
</tr>
<tr>
<td>J20050914</td>
<td>2005-09-14</td>
<td>Reflection on organization changes and current role and reporting structure</td>
<td>J20050914.doc</td>
</tr>
<tr>
<td>J20050918</td>
<td>2005-09-18</td>
<td>Reflection on reading J. Diamond’s “Collapse” and the relevance of its five-element framework in relation to information security risk management</td>
<td>J20050918.doc</td>
</tr>
<tr>
<td>J20051020</td>
<td>2005-10-20</td>
<td>Discussion notes on HKMA Banking Supervision and the CAMEL assessment process</td>
<td>OneNote20051020</td>
</tr>
<tr>
<td>J20051110</td>
<td>2005-11-10</td>
<td>Notes on dialectics on responsive security approach (with fellow practitioners)</td>
<td>OneNote20051110</td>
</tr>
<tr>
<td>J20051118-1</td>
<td>2005-11-18</td>
<td>Reflection on Responsive Security concept and its relation to People, Process, and Technology</td>
<td>OneNote20051118-1</td>
</tr>
<tr>
<td>J20051118-2</td>
<td>2005-11-18</td>
<td>Notes on awareness, competency and the idea of “habituation”</td>
<td>OneNote20051118-2</td>
</tr>
<tr>
<td>J20051209</td>
<td>2005-12-09</td>
<td>Reflection and notes on the safety road signs on the roads of New Zealand</td>
<td>OneNote20051209</td>
</tr>
<tr>
<td>J20051221</td>
<td>2005-12-21</td>
<td>Reflection and notes on the adoption of SSM as the underlying methodology for the Framework of Information Risk Management (FIRM)</td>
<td>J20051221.doc</td>
</tr>
<tr>
<td>J20060102</td>
<td>2006-01-02</td>
<td>Reflection and discussion notes on drills and rules (or policies) in relation to implementing responsive security</td>
<td>OneNote20060102</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>J20060104</td>
<td>2006-01-04</td>
<td>Discussion notes on the testing of responsive security strategy</td>
<td>OneNote20060104</td>
</tr>
<tr>
<td>J20060105-1</td>
<td>2006-01-05</td>
<td>Reflection on discussion with fellow Action Researcher on outcome</td>
<td>J20060105-1.doc</td>
</tr>
<tr>
<td>J20060105-2</td>
<td>2006-01-05</td>
<td>Reflection on the concept of &quot;State of Security Protection&quot;</td>
<td>OneNote20060105-2.doc</td>
</tr>
<tr>
<td>J20060106</td>
<td>2006-01-06</td>
<td>Discussion notes with fellow Action Researcher on research outcome</td>
<td>OneNote20060106</td>
</tr>
<tr>
<td>J20060108</td>
<td>2006-01-08</td>
<td>Discussion notes with fellow practitioner on details of information security framework</td>
<td>OneNote20060108</td>
</tr>
<tr>
<td>J20060113</td>
<td>2006-01-13</td>
<td>Reflection on how to respond to emerging security issues</td>
<td>OneNote20060113</td>
</tr>
<tr>
<td>J20060114</td>
<td>2006-01-14</td>
<td>Reflection on various IT security topics, FIRM, Piezoelectric theory, security certification, research issues, and thesis writing</td>
<td>J20060114.doc</td>
</tr>
<tr>
<td>J20060115</td>
<td>2006-01-15</td>
<td>Reflection on Petroski’s “To engineer is human” and the implication of engineering failures in relation to the concept of responsive security</td>
<td>J20060115.doc</td>
</tr>
<tr>
<td>J20060116</td>
<td>2006-01-16</td>
<td>Reflection on Responsive Security approach and the possibility of drawing parallels from other existing practices</td>
<td>J20060116.doc</td>
</tr>
<tr>
<td>J20060117-1</td>
<td>2006-01-17</td>
<td>Reflection on Responsive Security and its relation to maturity model approach</td>
<td>J20060117.doc</td>
</tr>
<tr>
<td>J20060122</td>
<td>2006-01-22</td>
<td>Reflection on Airlines mutual assistance in response to air traffic situations</td>
<td>OneNote20060122</td>
</tr>
<tr>
<td>J20060124</td>
<td>2006-01-24</td>
<td>Reflection on WMF Vulnerability security incident</td>
<td>OneNote20060124</td>
</tr>
<tr>
<td>J20060116</td>
<td>2006-02-16</td>
<td>Reflection and notes on limitation of current security and risk management approach</td>
<td>J20060216.ppt</td>
</tr>
<tr>
<td>J20060117-2</td>
<td>2006-02-17</td>
<td>Discussion notes (with fellow Action Researcher) on the needs for responsive security – from the viewpoint of inadequate coverage in current risk management approach</td>
<td>OneNote20060217</td>
</tr>
<tr>
<td>J20060118</td>
<td>2006-02-18</td>
<td>Reflection and notes on limitation of current security and risk management approach – refined descriptions and justification</td>
<td>J20060218.ppt</td>
</tr>
<tr>
<td>J20060123</td>
<td>2006-03-23</td>
<td>Updated presentation on need for responsive security strategy based on research findings and interpretation to-date</td>
<td>J20060223.ppt</td>
</tr>
<tr>
<td>J20060305</td>
<td>2006-03-05</td>
<td>Reflection and notes on limitation of current security and risk management approach – revised pictorial representation</td>
<td>J20060305.ppt</td>
</tr>
<tr>
<td>J20060306</td>
<td>2006-03-06</td>
<td>Reflection on discussion with an external information security professional on rapid response approach and intrusion prevention technology</td>
<td>J20060306.doc</td>
</tr>
<tr>
<td>J20060307</td>
<td>2006-03-07</td>
<td>Reflection and notes on meeting with another information security professional who thru’ his practice, discovered and promote the importance of experiential learning and scenario training.</td>
<td>J20060307.doc</td>
</tr>
<tr>
<td>J20060308</td>
<td>2006-03-08</td>
<td>Reflection and notes on information security readiness in a critical information infrastructure provider organization</td>
<td>J20060308.doc</td>
</tr>
<tr>
<td>J20060322</td>
<td>2006-03-22</td>
<td>Reflection and Discussion notes with Taxi driver on the notion that when system fails, it is not due to a simple error that just happened.</td>
<td>J20060322.doc</td>
</tr>
<tr>
<td>J20060327</td>
<td>2006-03-27</td>
<td>Reflection on various concepts and terminology relating to IRM practices</td>
<td>J20060327.doc</td>
</tr>
<tr>
<td>J20060328</td>
<td>2006-03-29</td>
<td>Notes on writing literature reviews</td>
<td>J20060328.doc</td>
</tr>
<tr>
<td>J20060402</td>
<td>2006-04-02</td>
<td>Reflection on Blakley’s paper on Information Risk Management</td>
<td>J20060402.doc</td>
</tr>
<tr>
<td>J20060406</td>
<td>2006-04-06</td>
<td>Reflection on the lack of consideration on the management aspect of information security risk</td>
<td>J20060406.doc</td>
</tr>
<tr>
<td>Reference</td>
<td>Date</td>
<td>Title</td>
<td>Source File</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>J20060717</td>
<td>2006-07-17</td>
<td>Notes and reflection on discussion with co-researcher on progress in IRM organization and practices, and evaluated changes in responsive approach undertaken in the company.</td>
<td>J20060717.doc</td>
</tr>
<tr>
<td>J20060721</td>
<td>2006-07-21</td>
<td>Notes and reflection on discussion with monetary authority on insider threats and Phishing issues.</td>
<td>J20060721.doc</td>
</tr>
<tr>
<td>J20060729</td>
<td>2006-07-29</td>
<td>Annotations of action research cycle 1 with data analysis and summary of issues and dilemmas.</td>
<td>DA1-20060729.doc</td>
</tr>
<tr>
<td>J20060819</td>
<td>2006-08-19</td>
<td>Annotations of action research cycle 2 with data analysis and summary of issues and dilemmas.</td>
<td>DA2-20060819.doc</td>
</tr>
<tr>
<td>J20060826</td>
<td>2006-08-26</td>
<td>Annotations of action research cycle 3 with data analysis and summary of issues and dilemmas.</td>
<td>DA3-20060826.doc</td>
</tr>
<tr>
<td>J20061029</td>
<td>2006-10-20</td>
<td>Updated report on results of Information Security Survey on External Organizations</td>
<td>Survey-20061020.doc</td>
</tr>
<tr>
<td>J20061126</td>
<td>2006-11-26</td>
<td>Annotations of action research cycle 4 with data analysis and summary of issues and dilemmas.</td>
<td>DA4-20061126.doc</td>
</tr>
</tbody>
</table>
Appendix C: Synthesis of information security approaches based on definition used

<table>
<thead>
<tr>
<th>Aspects of Information Security</th>
<th>Information Security Approaches</th>
<th>Use security technology</th>
<th>Baseline security</th>
<th>Risk-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Properties</td>
<td>Build security mechanisms to address each information security property or attribute, such as confidentiality, integrity, and availability, which is identified as part of the security requirements of the system.</td>
<td>Identify relevant security properties and assets that need protection across the organization, based mainly on business policies, and legal or regulatory requirements. Define minimum standards of protection required for each property across all systems.</td>
<td>Identify relevant security properties and assets that need protection across the organization, based on risk assessments.</td>
<td></td>
</tr>
<tr>
<td>Policies, Processes and Functionalities</td>
<td>Each security mechanism is mapped to specific security policy requirements, and processes are developed to facilitate the use of the security mechanism when dealing with information flow. The use of a security-focused software development method, including threat modeling, is also commonly promoted in this approach.</td>
<td>Define acceptable use policies for each security need, including provisions for exceptions where necessary. Define control objectives for each policy. Provide detailed procedure for achieving each control objectives.</td>
<td>Define security policies as part of the risk management or treatment process to address significant risk areas in the organizations. Define and develop security processes and functionalities as part of risk mitigation solutions for significant risk items.</td>
<td></td>
</tr>
<tr>
<td>Determining Priorities or Criticality</td>
<td>Priorities or criticality of each security technology or mechanism are determined by the security requirements, and often mapped to the level of assurance desired. For example, if the policy requires a high assurance system, those functions that are required for achieving the assurance certification will be given higher priority than those that are not.</td>
<td>All baseline requirements are given equal priority. They set the minimum standard that must be put in place as part of a system, for every system in the organization. If multiple baselines are specified for different business systems, priorities are normally aligned to the importance of each baseline or the systems involved.</td>
<td>Risk identification and analysis using quantitative or qualitative tools and methods, or a combination of both. Priorities determined based on risk analysis and assessment. High or critical risk items will get highest priority, followed by medium risk items. Low risk issues may be risk accepted, or given low priority for resolution.</td>
<td></td>
</tr>
<tr>
<td>Information Security Approaches</td>
<td>Use security technology</td>
<td>Baseline security</td>
<td>Risk-based</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------</td>
<td>-------------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>Aspects of Information Security</td>
<td>Similarly, requirements for complying with regulation or laws will be given higher priority and hence the selection and implementation of the related security technology.</td>
<td>Assortment of security techniques and mechanisms used, with preference for tried and tested methods, including procedural controls and technical controls. Use mostly security controls to prevent occurrence of undesired known adverse events.</td>
<td>Combination of security mechanisms and procedures for mitigating risks (high and medium risk items). For low risk items, may use procedural controls as compensating measures. Use of insurance as another method of managing risk in the form of liability transfer has also been suggested in some literature, but remains at the infancy stage.</td>
<td></td>
</tr>
<tr>
<td>Techniques to address security requirements</td>
<td>Techniques or measures applicable include many kinds of security technology, for example: (1) a secure operating systems, or trusted computing platform; (2) secure networking devices, such as a Firewall and a Virtual Private Network (VPN) gateway; (3) secure application programs; (4) data security programs (such as encryption programs); and (5) secure database systems.</td>
<td>Review and audit of actual implementation against baseline standards, using mainly pre-established checklists, and reviewers'/auditors’ knowledge, and experience.</td>
<td>Validation of risk assessment and treatment methods chosen. Review of implementation against risk treatment plan, either by self-checking or a third-party, or both at different times. Checklist remains as a popular tool for conduct of review and risk analysis.</td>
<td></td>
</tr>
<tr>
<td>Assurance</td>
<td>Assurance is based on formal certification or third-party technical reviews and testing. Standards such as the TCSEC (US-DoD, 1985) and Common Criteria (ISO/IEC, 2005b, 2005c, 2005d) to verify and validate the completeness and effectiveness of the security measures used to provide the security properties, secure or support the processes and functions, and address the priority threats and regulatory requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Summary of information security approaches based on five key aspects of the definition of information security
Appendix D: Framework for Information Risk Management

Framework for Information Risk Management

The framework for information risk management is based on the IT Security Standards Framework (SPRING Singapore, 2001) that I co-developed in 2001 (see Figure 35) as “a structure supporting or containing” the key areas that required identification and assessment as part of the security requirements definitions before designing the security plan (Princeton University, 2003). In accordance with the framework definition provided in the American Heritage® dictionary, the information security framework, in essence, encapsulates “a set of assumptions, concepts, values, and practices that constitutes a way of viewing reality” (Houghton Mifflin Company, 2000) in relation to the information security of the organization. The framework incorporated the learning and understanding gained since action research cycle 1 (Chapter 4), in particular, in the design of an information security risk management program in organization ALPHA.

The framework consists of seven components, which are the primary governing variables that influence the information risk management action strategy and plans. As such, it is also known as the “Framework for identifying information risk management governing variables”.

Each component has four parameters, namely, “input”, “output”, “outcome”, and “measure by”, to aid its identification, description, and subsequent design and implementation. A set of document templates was also designed for developing and documenting key deliverables of each component of the framework.

![Figure 35: Information Risk Management Framework](image)

The framework should be applied from top-down, beginning with the identification of relevant laws, regulations, and policies to the business to understand the boundary and constraints of the business and information security, and related compliance requirements. The objectives of this component are to determine (1) the governing rules and regulations, both internal and external to the organization, that influence the business, security programs and strategy of the organization; and (2) the required
security policies as part of the overall security strategy, based on an assessment of the related business and information risks that need to be addressed.

Besides the business rules, and related laws and regulations, the assessment should also consider external and internal risks factors (i.e., the threat environment), existing corporate business policies, new security policies that may need to be added or existing security policies that may be changed/deleted based on continuous risk assessment, changes in laws and regulations, and business environment.

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
<th>Outcome</th>
<th>Measure By</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Relevant laws and regulations;</td>
<td>• Threat Model</td>
<td>• Understanding of what’s at risk</td>
<td>• Level or extent of compliance required;</td>
</tr>
<tr>
<td>• Threat assessment</td>
<td>• Corporate Information Security</td>
<td>• Clarity of boundary of protection and risk management</td>
<td>Frequency of verification needed; Types of validation or certification of compliance.</td>
</tr>
<tr>
<td>• Business and Information Risk</td>
<td>Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Laws, Regulations, and Policies Parameters

Next is the Management and Organization structure currently established in the business, and any known plans for changes in the near future. The objectives are to (1) identify and define the desired management commitment, vision, and mission, objectives of security initiative/program, and organization structure to support its implementation; and (2) clarify roles and responsibilities, and financial model for security organization and programs delivery/implementation. In assessing this component, reflecting from the data analysis, the following questions were developed for considerations:

1. How are security managed in the organization? Are they going to be managed entirely internally, outsourced, or a hybrid of internal and external provisioning?

2. Who owns security responsibilities in the organization? Is there a security and/or privacy controller or chief information risk officer in the organization? What are her roles and responsibilities?

3. What is the organization reporting structure? Who does the security function reports into? Is the organization function for security based on a distributed, centralized, or hybrid model?

4. How is the security function supported financially? How would information security solutions be funded? Is it funded by the respective business unit, the corporate division, or a combination?

5. What is the process for establishing and gaining the financial and other resources required for information security in the organization? Are there any laws or regulations, or corporate policies governing this aspect of the organization?

6. What are the current practices in relation to the above questions?
Table 5: Management and Organization Parameters

Based on the two components above, with the list of output produced, achieving the desired outcome identified in the respective tables, the next step is to develop the security requirements specifications, which is the Security Services component of the framework.

The key component of the framework is the Information Security Services component, in which all other components are linked or supported. The set of information security services required should be based on the business requirements, which includes the short- and long-term plans of the business. Table 6 outlines the four parameters to be determined for the Information Security Services component.

Table 6: Security Services Parameters

Common information security services include identification and authentication, access control (or authorization), information confidentiality protection, information integrity protection, non-repudiation, accountability, and availability of systems, information, and people.

Depending on organization and country, personal data privacy protection may be an important requirement for the organization’s information security program. In such cases, privacy services may need to be identified and supported in addition to the information security services. Privacy services may include, for examples, clear notices, choice, data collection limitation, and data use control, as suggested by the local privacy regulation, or well-accepted international or regional framework, such as the APEC Privacy Framework (APEC-TEL, 2004b).

Following the identification of the information security services requirements, the next component to evaluate is the Methods and Processes being used in the
organization, as well as those that are required to support the implementation and operation of the information security services.

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
<th>Outcome</th>
<th>Measure By</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Requirements Specification;</td>
<td>• Security management blueprint - List of</td>
<td>• A management system in place to manage and monitor the security</td>
<td>• Security management reports</td>
</tr>
<tr>
<td>Security Acceptance Criteria</td>
<td>processes and methods for meeting</td>
<td>operations of the business and IT, providing ability to identify</td>
<td>• Readiness indicators, examples:</td>
</tr>
<tr>
<td></td>
<td>security services requirements</td>
<td>and response to emerging security issues and breaches, and</td>
<td>timeliness to apply security updates;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>addressing known security risks.</td>
<td>incident/alerts readiness and responsiveness</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(timeliness of response)</td>
</tr>
</tbody>
</table>

| Table 7: Methods and Processes Parameters |

Common methods and processes that are required include, but not necessarily limited to the following:

- Threat modeling and risk identification – essential to provide input to identification and prioritization of information security services
- Validation and assurance of completion of solutions and processes
- Risk monitoring, metrics, and indicators
- Secure baseline engineering and build process
- Application security development assurance process
- Incident response and handling
- Security update and change management
- Business continuity and disaster recovery planning and management
- Emergency communication and management
- Continuous awareness and education programs


The Methods and Processes component may be evaluated in parallel, before, or after the Techniques and Mechanisms component, which is based on the same set input documents. These two components should be integrated to ensure that there are adequate processes and methodologies for supporting the implementation and operation of the technical measures required and implemented, and wherever possible, technology is used to enable more automation to reduce human errors and improve efficiency and effectiveness of the information security systems.
<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
<th>Outcome</th>
<th>Measure By</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Requirements Specification;</td>
<td>• Security architecture blueprint</td>
<td>• An enterprise security system in place to provide the services required</td>
<td>• Completeness – gaps against requirements</td>
</tr>
<tr>
<td>Security Acceptance Criteria</td>
<td></td>
<td>to support the technical and management security requirements, ensuring</td>
<td>specification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>compliance with policy, and providing capability for ongoing security</td>
<td>• Residual risk indicators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>management.</td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Techniques and Mechanisms Parameters

In general, the technical and mechanisms component may be categorized into (1) infrastructure security systems, and (2) resource security systems. Infrastructure security systems are technical mechanisms that provide the foundation for implementing and achieving information security, which include:

- Authentication Systems;
- Authorization Systems;
- Audit/accounting Systems;
- Network Security Systems;
- Perimeter Isolation;
- Network Isolation;
- Host Isolation;
- Public Key Infrastructure (PKI) Systems, such as Certificate Authority, and Directory Services; and

Resource security systems are those that implement specific controls at the resources (including infrastructure such as network) to achieve the desired security properties as identified in the security services:

- Network access authorization/protection system;
- Information access authorization/protection services;
- Database access and security services; and
- Business applications access and security services.

Based on the output of the five components above, the next step is to make an assessment of available common practices and guidance to identify suitable standards and guidelines for comparison with existing and desired practices, and identify suitable practices for adoption and implementation, before devising specific technical mechanism or process design for in the action strategies for implementation. The
objectives of this component are to determine what others are the common practices, and what standards are available to meet the various needs in order to achieve:

- Better interoperability;
- Common baseline;
- Reduce errors; and
- Improve assurance.

The ISO/IEC 17799 standard (ISO/IEC, 2000, 2005e), amongst others, provides a useful reference for this component.

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
<th>Outcome</th>
<th>Measure By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management and Architecture blueprints</td>
<td>List of available guidance and best practices that could be adopted; and required</td>
<td>Clarity of detailed resources, steps, procedures, and configurations for implementation in security systems.</td>
<td>Awareness indicator, Practice/Efficacy measurement, Readiness indicators</td>
</tr>
</tbody>
</table>

Table 9: Guidelines and Common Practices

The final component is the technology and solutions to be designed and adopted for achieving the information security services, for implementing the technical mechanisms, methods, and processes devised in the earlier steps.

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
<th>Outcome</th>
<th>Measure By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management and Architecture blueprints</td>
<td>Physical security management and architecture design specification</td>
<td>Clarity of physical infrastructure and system, including details of resources required for implementation, maintenance and operations.</td>
<td>Cost efficacy, Extent/status of implementation, Readiness indicators</td>
</tr>
</tbody>
</table>

Table 10: Technology and Solutions Parameters

In this step, the existing and desired technology blueprints are identified and designed. The policies and implementation implications, in terms of resources, compliance, and timeliness are also assessed. Technology choice could be limited or affected by policies and regulations. Policies might also need to change or added to meet the challenges of using new technology selected for the implemented.
Bibliography


Denning, P. J. (2002). Career Redux - How can one design a career when career as an institution is dead? Entrepreneur has an answer". Communications of the ACM, 45(9), 21-26.


---

318


The Honeynet Project. (2002). *Know Your Enemy: Revealing the security tools, tactics, and motives of the Blackhat community:* Addison-Wesley.


