Information Security Management
Practices in Organisations

Moneer Alshaikh

Submitted in total fulfilment of the requirements of the degree of
Doctor of Philosophy

March 2018
School of Computing and Information Systems
The University of Melbourne
Abstract

Developing an information security capability is rapidly becoming a priority for organisations as security threats become more complex and sophisticated in the modern era. There has been much research aimed at developing information security tools and techniques to combat security threats. However, less research has focused on developing security management practice, a critical part of security capability.

This research project focuses on Information Security Management Practices (ISMPs), the set of strategic-level activities, including planning, organising, directing and controlling organisational resources (human, financial, physical and information) that are directed towards the application of managerial security controls in pursuit of information security objectives. In this thesis, three common deficiencies are identified in ISMP oriented guidelines and models for organisations. These three deficiencies are (1) poor conceptualisation around ISMP, (2) lack of comprehensive guidance on ISMP for organisations, and (3) lack of empirical work in the ISM area, more specifically in managerial practices. The three deficiencies identified constitute various aspects of a common problem: namely the lack of comprehensive, coherent and empirically tested guidance for organisations on information security management practices.

This thesis takes a managerial practice based perspective to investigate how organisations manage their information security program. The formal research question under investigation is: How can information security management be practiced in organisations? To answer this question, two sub-questions also are addressed:

1. How are Information Security Management Practices related to each other?
2. To what extent are Information Security Management Practices institutionalised in organisations?

The primary contribution of this thesis is the development of a rigorous, practice oriented, and empirically tested framework of information security management practices (ISMP). The proposed framework supports and guides organisations towards improving their management of information security. The framework was developed through a comprehensive review and analysis of the ISM literature. It was subsequently refined and validated qualitatively through thirty-four semi structured interviews with information security experts.
This research has four key contributions:

- The research provides the most complete, comprehensive and empirically backed framework of ISMPs for organisations; the framework complements fragmented best-practice advice on ISM in industry standards.
- The research project explains why organisations choose to adopt formal or informal approaches to the implementation of ISMPs and the consequences of adopting said approach.
- The research identifies the relationships between ISM areas, provides empirical evidence for the relationships, justifies the interdependencies between ISMPs, and explains the impact of inconsistent levels of quality among ISM practices.
- The research identifies a set of activities (Intra Organisation Liaison (IOL) management practices) undertaken by organisations to increase the level of stakeholder involvement and participation in the ISM process. The identification of the IOL management practices provides guidance to organisations on how to increase the level of stakeholders’ involvement and cultivate a culture of security.

The research contends that the management of information security program can be improved by: (1) implementing ISMPs in a holistic and comprehensive manner through using the proposed ISMP framework as standardized and formal checklist to benchmark and the ISMPs interdependencies framework; (2) assessing their current maturity level of the implementation of ISMPs and allocating the required resources to achieve more structured and formal implementation of ISMPs; (3) establishing formal communication process between security personnel and internal stakeholders through the implementation of IOL practices. This leads to effective management of information security where ISMPs are implemented in a holistic and collective manner with the support and participation of employees in the organisation.
DECLARATION

This is to certify that

i. the thesis comprises only my original work towards the PhD except where indicated in
   the Preface,

ii. due acknowledgement has been made in the text to all other material used,

iii. the thesis is less than 100,000 words in length, exclusive of tables, maps, bibliographies
    and appendices.

Signed by

Name: Moneer Alshaikh

Date:
ACKNOWLEDGEMENTS

First and foremost, I thank God for His never-ending grace, mercy and provision throughout this PhD journey and for giving me the strength and perseverance to complete the thesis.

I would like to express my sincere gratitude to my supervisors, Dr Sean Maynard, Dr Atif Ahmad, and A/Prof Shanton Chang for their relentless guidance and support throughout my candidature. Their insightful critiques, probing questions and constructive suggestions have shaped my approach to research in general. They have engaged me as a colleague and collaborator from the start, and their confidence in me has led me achieve far more than I had thought possible. I could not have imagined having better supervisors and mentors for my PhD study.

I would like to thank Prof Christopher Leckie the chair of my advisory committee for his comments and suggestions during my PhD committee meetings.

I would like to thank all the administrative staff and my colleagues in the School of Computing and Information Systems, University of Melbourne. Special thanks to Melbourne School of Graduate Research for organising PhD courses and workshops throughout my candidature.

I would like to thank my sponsor The University of Jeddah and Saudi Arabian Cultural Mission for their financial support and assistance to finish my study successfully. I am truly grateful for the phenomenal opportunity.

My thanks are also extended to the participants of my study for sharing their expertise and knowledge through the two rounds of the data collection.

I would like to thank my parents, my brothers and sisters, for their support and prayers.

Finally, my heartfelt appreciation to my wife Nawal for her patience, endorsement and motivation during my entire PhD journey. To my children, Naif, Noran and Rawan, thank you for your cheeky smiles and funny stories that always brighten up my stressful days.
PUBLICATIONS

The following are relevant workshops, and a conference presentation relating to this research project:


No substantial portions of text are shared verbatim between these works and the contents of this thesis.
# TABLE OF CONTENTS

Abstract.................................................................................................................................i
DECLARATION..........................................................................................................................iii
ACKNOWLEDGEMENTS..........................................................................................................iv
PUBLICATIONS .......................................................................................................................v
ABBREVIATIONS AND ACRONYMS..................................................................................xii

## Chapter 1 Introduction....................................................................................................1
1.1 Introduction ..................................................................................................................1
1.2 Study Background ........................................................................................................2
1.3 Research Problem .........................................................................................................3
1.4 Research Motivation .....................................................................................................5
1.5 Research Aims and Question .......................................................................................6
1.6 Scope of the Research ..................................................................................................7
1.7 Outline of Research Design ........................................................................................8
1.8 Overview of the Thesis Structure ..............................................................................9
1.9 Summary ......................................................................................................................12

## Chapter 2 Background..................................................................................................13
2.1 Introduction ..................................................................................................................13
2.2 An overview of information security .........................................................................13
2.3 Information security management practices (ISMPs) .................................................14
  2.3.1 Professional literature ..............................................................................................15
  2.3.2 Academic literature ................................................................................................17
  2.3.3 Existing studies on ISMPs .......................................................................................18
  2.3.4 Analysis of the existing models and frameworks ..................................................23
2.4 The identification of the research problem ..................................................................24
  2.4.1 Deficiency 1: Poor conceptualisation around ISMPs ...........................................24
  2.4.2 Deficiency 2: The lack of comprehensive guidance on ISMPs for organisations .26
  2.4.3 Deficiency 3: the lack of empirical work in the ISM area more specifically into the
                  managerial practices ..............................................................................................28
2.5 Summary ......................................................................................................................29

## Chapter 3 Research Design ..........................................................................................30
3.1 Introduction ..................................................................................................................30
3.2 Research characteristics of this study .......................................................................30
  3.2.1 Research paradigm ..................................................................................................30
  3.2.2 Nature of this research ...........................................................................................31
  3.2.3 The role of information systems theories ...............................................................31
  3.2.4 Research methods ..................................................................................................34
3.3 Research Design ..........................................................................................................35
  3.3.1 Phase 1: Contextual study ......................................................................................36
  3.3.2 Phase 2: Conceptual study .....................................................................................36
  3.3.3 Phase 3: Empirical study .......................................................................................36
3.4 The Conceptual Study ................................................................................................37
  3.4.1 Literature analysis and knowledge synthesis ...........................................................38
3.5 Empirical study ...........................................................................................................39
  3.5.1 Interviews ................................................................................................................39
  3.5.2 Final validation (Follow up interviews) .................................................................43
3.6 Data analysis ................................................................................................................43
Chapter 6 Information Security Policy Management Practices .............................................. 98
  6.1 Introduction .................................................................................................................. 98
  6.2 Literature review ......................................................................................................... 98
    6.2.1 Models of ISP development .................................................................................. 99
    6.2.2 Stakeholders Involvement .................................................................................... 105
    6.2.3 Compliance .......................................................................................................... 105
    6.2.4 Information security policy quality ....................................................................... 106
  6.3 Information Security Policy Management Practice framework ....................................................... 107
    6.3.1 The Development stage ......................................................................................... 108
    6.3.2 The Implementation and Maintenance Stage ....................................................... 112
    6.3.3 The Evaluation Stage ........................................................................................... 115
  6.4 Data Analysis and Findings ......................................................................................... 116
    6.4.1 The development stage ......................................................................................... 117
    6.4.2 The Implementation & Maintenance Stage .......................................................... 122
    6.4.3 The Evaluation Stage ........................................................................................... 125
    6.4.4 Summary of the findings ..................................................................................... 126
  6.5 Final validation ............................................................................................................ 128
  6.6 Discussion .................................................................................................................... 129
    6.6.1 Formal versus informal approach to the implementation of ISP management practices .. 129
    6.6.2 Stakeholders’ involvement in the process ............................................................. 130
Chapter 9 Information Security Intra-Organisational Liaison Management Practices 203

9.1 Introduction .............................................................................................................. 203
9.2 Literature Review .................................................................................................... 204
  9.2.1 Stakeholders’ involvement in the information security management process .... 204
  9.2.2 Communication between the information security team and internal stakeholders .... 205
9.3 Towards a Model of Intra-Organisational Liaison Management Practice .......... 208
  9.3.1 Internal communication in the organisational communication literature .......... 209
  9.3.2 Recommendations for effective communication and stakeholders’ involvement in ISM literature ........................................................................................................ 211
  9.3.3 Why InfoSec IOL differs from general IOL/ org communication ...................... 212
9.4 Data analysis and Findings ....................................................................................... 213
  9.4.1 The development stage ..................................................................................... 214
  9.4.2 The Implementation & Maintenance Stage ....................................................... 219
  9.4.3 The Evaluation Stage ....................................................................................... 221
9.5 Final Validation ........................................................................................................ 223
9.6 Discussion ................................................................................................................ 225
  9.6.1 An institutionalisation of the communication process ...................................... 225
  9.6.2 Communication with stakeholders .................................................................. 226
  9.6.3 The role of IOL management practices in cultivating a security culture .......... 227
  9.6.4 Stakeholders involvement in ISMPs ................................................................. 230
  9.6.5 Provide further guidance to increase the level of stakeholders’ involvement (stakeholders matrix) ................................................................. 231
  9.6.6 Evaluating IOL management practices ............................................................ 235
9.7 Summary .................................................................................................................. 235

Chapter 10 Discussion & Conclusions ......................................................................... 236

10.1 Introduction ............................................................................................................ 236
10.2 Project Overview .................................................................................................... 236
10.3 Answers to the Research Questions ...................................................................... 238
  10.3.1 Primary research question: How can information security management be practised in organisations? ................................................................. 238
  10.3.2 Supporting research question 1: How are Information Security Management Practices related to each other? ........................................ 241
  10.3.3 Supporting research question 2: To what extent are information security management practices institutionalised in organisations? .... 252
10.4 Contributions ........................................................................................................ 254
  10.4.1 Contributions to theory ................................................................................ 255
  10.4.2 Implications for Practice .............................................................................. 256
10.5 Limitations ............................................................................................................ 259
10.6 Future Research .................................................................................................... 261
10.7 Conclusion ............................................................................................................. 262

References .................................................................................................................... 264

APPENDIX A: RESEARCH METHODOLOGY DOCUMENTATION 288

  Ethics Approval ......................................................................................................... 288
  Plain Language Statement ..................................................................................... 289
  Consent Form ........................................................................................................... 290
  Interview Protocol ................................................................................................. 291

APPENDIX B: REPRESENTATIVE EVIDENCE FOR INTERDEPENDENCIES BETWEEN ISMPs .................................................................................................................. 292
LIST OF TABLES

TABLE 2-1 : SUMMARY OF ISM PROCESSES ................................................................. 20
TABLE 2-2 ANALYSIS OF COMMON ISMP AREAS IN EXISTING ISM LITERATURE .......... 22
TABLE 2-3 SUMMARY OF THE EXISTING ISM FRAMEWORKS AND MODELS IN RELATION TO THE THREE IDENTIFIED DEFICIENCIES. ................................................................. 24
TABLE 3-1 BACKGROUND INFORMATION ABOUT THE STUDY PARTICIPANTS ............... 42
TABLE 4-1 SUMMARY OF LITERATURE REVIEW OF ISMPs ........................................... 51
TABLE 4-2 THE TOP-LEVEL OF THE PRELIMINARY FRAMEWORK OF ISMP ..................... 57
TABLE 5-1 THE PRELIMINARY FRAMEWORK OF ISTA MANAGEMENT PRACTICES ............ 65
TABLE 5-2 EXAMPLE OF THE ISRM PROCESS STAKEHOLDERS AND THEIR ROLES .......... 69
TABLE 5-3 TEAM MEMBERS AND THEIR RESPONSIBILITIES ........................................... 71
TABLE 5-4 SUMMARY THE DATA THAT NEED TO BE COLLECTED ...................................... 73
TABLE 5-5 ISRM TREATMENT OPTIONS ........................................................................... 74
TABLE 5-6 ISRM PRACTICES AND NUMBER OF PARTICIPANTS THAT SUPPORT PRACTICES ...... 78
TABLE 5-7 THE REFINED FRAMEWORK OF ISRM PRACTICES ........................................... 90
TABLE 6-1 DEFICIENCIES IDENTIFIES IN EXISTING POLICY DEVELOPMENT LIFECYCLES .......... 103
TABLE 6-2 INFORMATION SECURITY POLICY MANAGEMENT PRACTICES FRAMEWORK ....... 108
TABLE 6-3 SUMMARY OF SECTIONS AND ATTRIBUTES OF SECURITY POLICY DOCUMENTS ...... 112
TABLE 6-4 POLICY MANAGEMENT PRACTICES AND NUMBER OF PARTICIPANTS THAT SUPPORT THESE PRACTICES ............................................................................ 117
TABLE 6-5 THE REFINED FRAMEWORK OF POLICY MANAGEMENT PRACTICES ................... 127
TABLE 7-1 A COMPARISON BETWEEN ISTA PROGRAM’S ELEMENTS ADOPTED .................. 137
TABLE 7-2 THE PRELIMINARY FRAMEWORK OF ISTA MANAGEMENT PRACTICES .............. 143
TABLE 7-3 SUMMARY OF THE ISTA PROGRAM’S KEY ROLES AND THEIR RESPONSIBILITIES .... 146
TABLE 7-4 EXAMPLE OF GROUPS THAT CAN BE TARGETED FOR ISTA PROGRAM .............. 148
TABLE 7-5 SUMMARY OF THE MOST COMMON DELIVERY METHODS ADOPTED FROM ........... 150
TABLE 7-6 ISTA PRACTICES AND NUMBER OF PARTICIPANTS THAT SUPPORT PRACTICES ...... 154
TABLE 7-7 THE REFINED FRAMEWORK OF ISTA MANAGEMENT PRACTICES ....................... 164
TABLE 8-1 THE PRELIMINARY FRAMEWORK OF ISIR MANAGEMENT PRACTICES ................ 164
TABLE 8-2 ISIR PRACTICES AND NUMBER OF PARTICIPANTS THAT SUPPORT PRACTICES ....... 175
TABLE 8-3 THE REFINED FRAMEWORK OF ISRM PRACTICES ............................................ 186
TABLE 9-1 SUMMARY OF STAKEHOLDERS’ INVOLVEMENT IN ISMPs FROM THE LITERATURE 206
TABLE 9-2 INTERNAL COMMUNICATION MATRIX ADOPTED FROM .................................. 210
TABLE 9-3 INFORMATION SECURITY IOL MANAGEMENT PRACTICES ............................... 214
TABLE 9-4 POLICY MANAGEMENT STAKEHOLDER MATRIX .............................................. 232
TABLE 9-5 RISK MANAGEMENT STAKEHOLDER MATRIX ......................................... 233
TABLE 9-6 ISTA MANAGEMENT STAKEHOLDER MATRIX ......................................... 234
TABLE 9-7 INCIDENT RESPONSE MANAGEMENT STAKEHOLDER MATRIX ................. 234
TABLE 10-1 THE ISMP FRAMEWORK - PRACTICE LEVEL ...................................... 238
TABLE 10-2 SUMMARY OF THE RESEARCH CONTRIBUTIONS AND THEIR IMPLICATIONS .... 254

LIST OF FIGURES

FIGURE 1-1 A THREE-PHASE RESEARCH DESIGN .................................................. 9
FIGURE 1-2 OVERALL STRUCTURE OF THE THESIS ............................................ 11
FIGURE 2-1 INFORMATION SECURITY TRIPLET MODEL ADOPTED .......................... 14
FIGURE 3-1 SUMMARY OF THE RESEARCH DESIGN .......................................... 35
FIGURE 4-1 PRELIMINARY CONCEPTUAL FRAMEWORK OF ISM PROCESS IN ORGANISATIONS .... 46
FIGURE 6-1 PFIRE'S CONCEPTUAL FRAMEWORK PROPOSED ................................ 101
FIGURE 10-1 THE OVERALL ISMP'S DEPENDENCIES FRAMEWORK ....................... 243
FIGURE 10-2 RISK MANAGEMENT CENTRED INTERDEPENDENCIES ....................... 244
FIGURE 10-3 INCIDENT RESPONSE MANAGEMENT CENTRED INTERDEPENDENCIES ........ 247
FIGURE 10-4 ISTA MANAGEMENT CENTRED INTERDEPENDENCIES ....................... 250
## ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ISM</td>
<td>Information Security Management</td>
</tr>
<tr>
<td>ISMP</td>
<td>Information Security Management Practice</td>
</tr>
<tr>
<td>ISP</td>
<td>Information Security Policy</td>
</tr>
<tr>
<td>SETA</td>
<td>Information Security Education, Training and Awareness</td>
</tr>
<tr>
<td>ISTA</td>
<td>Information Security Training and Awareness</td>
</tr>
<tr>
<td>ISRM</td>
<td>Information Security Risk Management</td>
</tr>
<tr>
<td>ISIR</td>
<td>Information Security Incident Response</td>
</tr>
<tr>
<td>ISIRT</td>
<td>Information Security Incident Response Team</td>
</tr>
<tr>
<td>IOL</td>
<td>Intra Organisation Liaison</td>
</tr>
</tbody>
</table>
Chapter 1 INTRODUCTION

1.1 Introduction
This thesis investigates the management practices of information security in organisations with the aim to develop a comprehensive framework to benefit organisations. Research on information security management (ISM) has acknowledged the important role that management practice plays in protecting organisations from a wide range of information security risks. Much research has been published on managerial-level security controls such as policy, risk, awareness and incident response however the literature is fragmented and does not investigate the collective management practices that organisations should institute for information security purposes (Soomro, Shah, & Ahmed, 2016; Zafar, Ko, & Clark, 2014). Such a framework is extremely important for providing organisations with guidance on implementing managerial controls that enable them to manage their information security effectively.

Hence, this thesis develops a rigorous, practice oriented, and empirically tested framework of information security management practices (ISMPs) to benefit organisations.

This chapter provides an overview of the research project and the main elements of the thesis. The chapter starts by providing background to the research project and the research motivations and aims. Subsequently, the chapter presents the research problem, outlines the current state of the research and identifies gaps. The chapter also presents the research questions, the contributions of the research, the scope of the study, the research design and the structure of the thesis.
1.2 Study Background

Over the past two decades, information security has become one of the top priorities for organisations. Organisations are very dependent on their information systems. In order to gain a competitive advantage in the business world, organisations need to share information and make it available to employees, business partners and customers beyond their traditional boundaries. The increase in the need to share information and the adoption of new technologies have made maintaining security a very challenging task. In order to protect their information, organisations implement technological-based solutions.

Organisations rely on the implementation of technological controls to improve security (Balozian & Leidner, 2017; Soomro et al., 2016). Although the implementation of technological controls is important, relying on technological solutions is inadequate for mitigating risk, as recent security reports show that the number of security incidents is increasing (Australian Cyber Security Centre, 2016; Crowd Research Partners, 2017; SANS, 2017).

The increase in the number of security incidents in organisations suggests that technological controls are not sufficient to prevent risk. It also shows that perceiving information security as a technological problem represents a very limited understanding of the security problem. Several researchers (e.g., Niemimaa & Niemimaa, 2017; Soomro et al., 2016; Whitman & Mattord, 2014) argue that the security problem should be approached in a more comprehensive manner, and combinations of managerial controls and technological controls should be applied to solve the problem. (Hu, Dinev, Hart, & Cooke, 2012; Hu, Hart, & Cooke, 2007; Soomro et al., 2016) argue that good management practices are as important as the implementation of technological controls for providing better protection for organisational information assets.

The focus of the research has shifted towards the socio-technical aspects of information security. The importance of good management practices for protecting organisational resources has also been recognised. Consequently, much research has been done on the non-technological aspects of security. For example, there is a considerable body of literature that highlights the importance of security policy and its role in a security program, security risk management, security awareness, incident response, a security culture and top management involvement in security. Further, professional standards such as IED/ISO 27000 series have been developed to assist organisations to establish good information security management.

Both academic and professional publications on the managerial aspect of information security are limited to certain aspects of managerial controls and do not provide comprehensive guidance.
on the complete range of ISMPs. Hence, the literature does not provide sufficient guidance on the managerial aspect of information security. More analysis of the literature is provided in section 2.3.

The consequences of inadequate managerial guidance on information security are significant for modern organisations given the significant exposure to security threats. Organisations embarking on a program of information security management have insufficient guidance on what methods can be implemented to meet security objectives. Further, organisations have no widely accepted benchmark (backed by empirical evidence) against which improvement in existing management practices can be assessed.

Therefore, this study aims to develop comprehensive guidance for organisations on what information security management practices should be implemented to protect their information resources.

1.3 Research Problem

Securing information resources is an important challenge for organisations as the threat landscape evolves and incidents escalate. The information resources of an organisation are susceptible to an increasingly wide range of threats, such as leakage of trade secrets and intellectual property, disruption of mission-critical systems and malicious attack from both insiders and outsiders, resulting in significant impact on business continuity. To address these security threats, organisations implement information security programs that consist of a range of technological controls and managerial practices.

Most organisations seek guidance on how to implement an information security program from industry standards (e.g. ISO/IEC 27000 series, NIST publications and SANS publications). These standards provide advice to assist organisations to develop their information security program by suggesting a ‘mixed bag’ of processes, practices and controls that organisations should implement to protect their information resources.

Although these standards have been subject to considerable refinement over the years, Siponen and Willison (2009) point out that the standards (1) remain abstract and generic, focusing on the existence of security processes and providing little advice on (managerial) practice, and (2) provide no evidence of having been empirically validated to the extent that they are a reliable source of advice to organisations. Consequently, the guidance that existing industrial standards and best-practice guidelines provide to organisations on the range of ISMPs is limited.
The responsibility of providing practice-oriented and empirically backed guidance falls to information systems researchers (rather than more technologically centred computing researchers). However, the discourse on information security management practices (ISMPs) is fragmented and dispersed and does not build cumulatively on prior knowledge. Madnick (1978) suggests that the managerial aspects of information security are “largely diffuse and unorganised” (p.61). Even though this was written more than 30 years ago, it still holds true, with even more prominence in the current environment than ever before. For instance, several researchers argue that ISM is a relatively immature discipline and that more research is needed to explore challenges and deficiencies, identify best practices and develop comprehensive frameworks/methodologies for the management of information security (Choobineh, Dhillon, Grimaila, & Rees, 2007; Lim, Chang, Ahmad, & Maynard, 2012; Soomro et al., 2016; Zafar & Clark, 2009; Zafar et al., 2014).

The lack of maturity is rooted in the reliance on an informal view of ISMPs and also due to the lack of consensus on key terms and concepts. The literature pertaining to the ISM domain is fragmented and not cumulative, as there is no consensus on foundational principles and concepts, and it does not present a coherent view of practices. Hence, the ISM literature does not offer a widely accepted and precise view on ISMPs.

Part of the reason for this is because much of the research in the information systems domain around ISM has remained disengaged from the inner workings of management practice in organisations (e.g. variance models tested using surveys). The majority of the research effort in the ISM domain has focused on studying individual (as opposed to collective) aspects of ISM and applying theories drawn from reference disciplines. Theory building, and theory-testing research have implications for practice in organisations; however, the aim of this type of research is not to provide guidance on ISMPs.

Given industry standards provide little (evidenced) advice on practice, and that systemic issues with practice are reported in the literature as a primary reason for the ineffectiveness of ISM, this thesis points out that the field of ISM cannot progress without agreement on what constitutes ISM. Therefore, this research asks the question: How can information security management be practised in organisations?
1.4 Research Motivation

The motivation behind this research project is the paucity of rigorous, comprehensive and empirically evidenced guidance for organisations on information security management practices (ISMPs). The review of the ISM literature has identified three key deficiencies regarding ISMPs (see Section 2.4).

The first deficiency is the poor conceptualisation around information security management practices (ISMPs). The review of the literature revealed several indications of the immaturity of the domain and the poor conceptualisation around ISMPs. These indications are lack of definition of ISMPs, lack of a consensus on terminology around management practice that is used across the literature, and lack of consistent and systematic classification of ISMPs in both the academic and professional literature.

The second deficiency is the lack of comprehensive guidance on ISMPs for organisations. Several researchers have cited the lack of comprehensive work in the ISM area and the need for a holistic and comprehensive approach (Lim et al., 2012; Soomro et al., 2016; Zafar & Clark, 2009; Zafar et al., 2014). For example, Zafar and Clark (2009) and Zafar et al. (2014) state that information security is widely regarded as a field that lacks comprehensive research. Several researchers highlight the importance of a comprehensive and holistic approach for information security management (Eloff & Eloff, 2003; Soomro et al., 2016; Swanson & Guttman, 1996). For example, Dhillon (2007a) argues that an effective information security management program should integrate different information security processes, such as information security risk management, educating personnel in information security awareness and establishing and executing information security policies.

The third deficiency is the lack of empirical work in the ISM area, more specifically in the area of managerial practices. Much of the existing work on ISMPS has been based on conceptual analysis and the opinion of industry professionals, with very little empirical evidence presented to justify the recommended practices (Ezingeard & Bowen-Schrire, 2007; Qingxiong, Johnston, & Pearson, 2008; Siponen, 2005; Tryfonas, Kiountouzis, & Poulymenakou, 2001). In the past decade, more empirical research has been conducted in various areas of ISM. However, much of the empirical research has focused on using theories and developing frameworks for various aspects of ISM rather than providing empirically evidenced guidance on ISMPs. Additionally, organisations rely on ISM industry standards to guide them in managing their information security programs. However, as previously mentioned, these standards are not based on
empirical evidence and do not provide any justification for how the recommendations were identified (Siponen & Willison, 2009). Dhillon, Tejay, and Hong (2007) and Dhillon and Backhouse (2001) argue that the lack of empirical work has resulted in a limited understanding of what ISM involves, which has led to insufficient guidance on the ISMPs that the organisations should implement.

This thesis argues that these three deficiencies in the literature have resulted in insufficient guidance for organisations on the range of ISMPs that should be implemented to preserve their information resources. The consequences of inadequate managerial guidance on information security are significant for the modern organisation, given the significant exposure to security threats. Therefore, it is vital to develop coherent, comprehensive and empirically tested guidance to organisations on the managerial practices of information security.

1.5 Research Aims and Question

Effective security management is very critical for protecting organisational information resources. A precursor to effective information security management in organisations is implementation of good ISMPs. Therefore, this research project aims to provide organisations with guidance on the range of ISMPs that can be implemented. The research will address the deficiencies in the literature by developing a comprehensive framework of ISMPs that:

- assists organisations to effectively implement ISMPs by providing coherent guidance on the range of ISMPs across various information security management areas
- enables organisations to assess their implementation of ISMPs by using the proposed framework as a benchmark.

Hence, an essential aim of this research is to assist security managers to successfully manage their security program through the implementation of good ISMPs. More specifically, the research in this thesis aims to:

➢ identify information security management practices? from the literature
➢ develop and validate a comprehensive framework of ISMPs
➢ improve information security by promoting the implementation of good information security management.

To achieve the aims identified above, the overarching and primary research question that the research seeks to answer is:
How can information security management be practised in organisations?

Secondary research questions are:

1. How are information security management practices related to each other?
2. To what extent are information security management practices institutionalised in organisations?

1.6 Scope of the Research

Information security is a multidimensional (technological, socio-technological and management). This research investigates information security from a management practice perspective. The strategic level of management activities that are undertaken by security managers will be the focus of this thesis.

The literature (academic and professional) does not provide a formal definition for the term information security management practices (ISMPs) and what it involves. The word ‘practice’ is defined by Wenger, McDermott, and Snyder (2002) as a set of socially defined ways of doing things in a specific domain. Practices are concrete and observable and underpinned by the skills, knowledge and experiences of organisational participants (Newell, Tansley, & Huang, 2004; Von Krogh, Haefliger, Spaeth, & Wallin, 2012). The notion of practice is therefore useful for exploring how work is actually done by individuals and groups in a specific context (Ashurst, Doherty, & Peppard, 2008).

Practices in the information security domain are the set of activities undertaken to protect organisational resources. These activities have two different levels of analysis: operational and strategic (Choobineh et al., 2007). Operational-level activities are concerned with the configuration, implementation, and monitoring of technological controls, while strategic-level activities involve things like the development, implementation, and evaluation of ISP, security education, training and awareness program.

Therefore, this research defines the term information security management practices (ISMPs) as the set of strategic-level activities, including planning, organising, directing and controlling organisational resources (human, financial, physical and information) that are directed towards the application of managerial security controls in pursuit of information security objectives.
This research focuses on the managerial practices of information security. The research project takes a management perspective in that it seeks to understand how information security is managed in organisations. The proposed model of ISMP is intended to be generic, unconstrained by the type and the size of organisation or circumstances of any specific jurisdiction, so that it can be used by a wide audience. Nevertheless, the model can be customised for certain contexts in future research as discussed in the concluding chapter (Chapter 10).

Following are scope definitions of key concepts related to the research project:

1. Organisations: All kinds of organisations in both the public and private sectors.
2. Information security: The protection of organisational information assets (that include the information and the systems) from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
3. Information security management: The process of applying formal, informal and technological controls with the objective of protecting the confidentiality, integrity and availability of information in the physical and digital environment whilst maintaining strategic alignment with the organisational mission.

**1.7 Outline of Research Design**

Due to the explorative nature of this study, the research project follows a qualitative research design. As depicted in Figure 1-1, this project consists of three studies: a contextual study, a conceptual study and an empirical study.

The **contextual study** involves conducting a conventional literature review to develop an understanding of the ISM area and identify gaps and limitations in the area in regard to managerial practices.

In the **conceptual study**, the relevant literature on ISM is comprehensively reviewed based on (Okoli & Schabram, 2010) approach. The grounded theory analysis process (Neuman, 2013; Wolfswinkel, Furtmueller, & Wilderom, 2013) was followed to analyse the literature. The findings of this phase have led to a research framework for ISMPs that can be implemented by organisations to safeguard their information assets.
The empirical study aims to validate and refine the proposed conceptual framework. This phase consists of two sequential rounds of data collection. First, semi-structured interviews with security experts and leaders in the industry are conducted to refine the preliminary framework of ISMPs. Second, follow-up interviews are conducted with the same participants for final validation of the proposed framework.

1.8 Overview of the Thesis Structure

This thesis consists of ten chapters (see Figure 1-2):

- **Chapter 1 Introduction**: (as discussed here) Gives a brief background of the research problems, provides the research questions, explains the contribution of the research and provides the thesis structure.
- **Chapter 2 Background**: Provides an overview of the literature on information security management and the existing standards and frameworks, and also outlines the deficiencies in the literature.
- **Chapter 3 Research Design**: Explains the research design used in this research and provides justification for the research paradigm, research method, data collection, analysis techniques and tool.
➢ **Chapter 4 Research Conceptual Framework**: Describes the development process of the research conceptual framework. This includes providing a detailed explanation of the process used to analyse the literature and a description of the top-level structure of the proposed framework.

➢ **Chapter 5, Chapter 6, Chapter 7 and Chapter 8**: These four chapters are dedicated to areas of ISMPs (risk management, policy management, ISTA management and incident response management) that have been identified through the analysis of the literature described in Chapter 4. Each chapter consists of five main parts:

- Part 1: Literature review of the area, which provides an overall description of the state of the research in the area and a review of the existing models, frameworks and guidelines, with the aim of providing guidance to organisations on the range of management practices that should be implemented to manage each area. This part also outlines gaps in the literature of each area in relation to ISMPs.

- Part 2: Framework development, which describes the synthesis of the existing literature of the area around the ISMP.

- Part 3: Data analysis and findings, which present the analyses of the empirical data collected through semi-structured interviews with information security experts to validate the framework developed in Part 2.

- Part 4: Final validation, which presents the analyses and findings from the followup interviews that were conducted to validate the framework of each ISMP area.

- Part 5: Discussion of the findings and the contribution to the existing literature of each particular area. An overall discussion will be presented in Chapter 10.

➢ **Chapter 9 Information Security Intra Organisation Liaison (IOL) Management Practices**: During the analysis of the empirical data, the research realised that a successful implementation of practices within each area (Chapters 5–8) depends heavily on the effective participation of relevant internal stakeholders. However, the review could not find practice-based guidance for security professionals on how to communicate effectively with internal stakeholders to increase their participation in the ISM process. This chapter addresses the gap in the literature by reviewing the need for communication and creation of general organisational communication literature. The chapter also presents IOL practices reported by the participants and discusses how these practices can increase the participation
of internal stakeholders. Furthermore, it demonstrates how IOL practices assist in building a security culture in organisations.

- **Chapter 10 Discussion & Conclusions:** Provides an overall discussion of the key findings of the research and refines the research framework. The chapter also concludes the thesis answering the research questions, presenting the contributions to theory and practice, and outlining both the limitations associated with this research and the recommendations for future research.

![Overall Structure of the thesis](image)

**Figure 1-2 Overall Structure of the thesis**
1.9 Summary

In this chapter, the research project was introduced, including the research problem, research question, aim and scope of the research, research approach and thesis structure. The next chapter provides background information about the area and discusses deficiencies in the existing literature on ISMP.
Chapter 2 BACKGROUND

2.1 Introduction
The majority of literature in information security management (ISM) seeks to make knowledge contributions to a single practice area whether it is policy, risk management, or incident response, whereas this research project seeks to make knowledge contributions to ISMPs collectively. This chapter provides an overview of the research area with more extensive reviews each ISMP area being presented within Chapters 5 to 8.

The purpose of this chapter is to:
1. present an overarching view of information security as the background context of this research
2. highlight the importance of managerial practices within Information Security
3. contextualise the gap that this research addresses within the context of information security

2.2 An overview of information security
From an information systems perspective, information security can be characterised as the relationship between three key components: information resources, threats, and controls (see Figure 2-1) (Baskerville, 2005). Information resources refer to assets that have value and, therefore, need to be protected. Organisations aim to preserve the confidentiality, integrity and availability of their information resources (referred to as the CIA triangle) (Baskerville, 2005). In addition to the CIA triangle, other properties can include authenticity, accountability, non-repudiation, and reliability (ISO/IEC27002, 2006; Whitman & Mattord, 2011). Any causal factor that can affect information security properties in regard to information resources is considered a threat (Dhillon, 2001). Information security threats can be purposive or incidental in nature (Guo, 2013), and may include information disclosure, denial of service, and integrity violation (Dhillon, 2001).
To protect information resources from threats, organisations implement a range of protective measures referred to as controls, which can be formal controls, informal controls, technological controls (Sveen et al., 2009, Dhillon and Torkzadeh, 2006). Formal controls are developed in response to findings from risk assessments and audits, and are essentially prescriptive. They include policies and procedures that provide advice to personnel on the one hand and outline punitive measures for non-compliance on the other. Informal controls include training and education that influence security culture, and are essentially suggestive. Technological controls are restrictive in nature and include firewalls, intrusion detection systems, and other such devices that regulate access to resources (Dhillon, 2001). Practices exist for the management of all these types of controls.

2.3 Information security management practices (ISMPs)

Information security management (ISM) refers to the structured process for the implementation and ongoing management of information security in organisations (Savola, Anttila, Sademies, Kajava, & Holappa, 2006). ISM aims to achieve and maintain adequate levels of confidentiality, integrity and availability of information resources (Whitman & Mattord, 2011). Cavalli, Mattasoglio, Pincioli, and Spaggiari (2004) assert that ISM is the process of planning, organising and commanding, coordinating, and controlling in order to establish an adequate level of security.

The majority of the research in the information security domain has been done in technological aspects of information security (Chaudhry, Chaudhry, & Reese, 2012; Ezingeard & Bowen-
However, in the two last decades, there has been increased interest in managerial aspects of information security and the influence they have on the organisational context (Oyelami & Ithnin, 2015; Polónia & Sá-Soares, 2013; Soomro et al., 2016). The increase in information security incidents, despite the implementation of technological controls, has made academics and practitioners realise that information security is not an exclusively technological problem but also has a managerial dimension (Ahmad, Bosua, & Scheepers, 2014; Ruighaver, Maynard, & Chang, 2007). In addition, the implementation of technological controls depends on information security policy and organisational strategies (Soomro et al., 2016). Many authors argue that a comprehensive information security program must include technological controls and good management practices (Dhillon 1997; Borodzicz 2005; Whitman and Mattord 2005; Slay and Koronios 2006 Hu, Hart and Cooke 2007).

Information security management practices (ISMPs) play a significant role in the protection of information resources in organisations (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Chaudhry et al., 2012). Whilst there has been a considerable research on the technological and managerial aspects of information security, the literature does not specifically investigate the collectives set of practices around the three types of controls. Therefore, there is a need for sufficient and coherent guidance for organisations on the range of managerial practices that should be implemented to protect their information resources.

The existing literature on ISMPs can be divided into either academic or professional literature. In the remainder of this section, this research reviews the existing professional and academic literature on the topic of managerial practices in information security.

2.3.1 Professional literature

Professional literature consists of industrial standards and best-practice guidelines which play a major role in the information security domain (A. Ahmad, 2010; AS/NZS ISO/IEC 27005:2012; Ronald S Ross, 2009). They provide considerable advice to assist organisations to develop their information security program by suggesting a mixed bag of managerial practices and technological controls that organisations should implement to protect their information resources (Goldes, Schneider, Schweda, & Zamani, 2017; von Solms & von Solms, 2018).

There are many best-practice standards that have been proposed by several organisations and government agencies. These standards and best practice guidelines can be divided into two types
according to their aims: (1) provide overall guidance to organisations on how to develop an effective information security program, and (2) provide guidance to organisations on a specific area of ISM such as information security policy (Diver, 2007; SANS Institute, 2001), information security risk management (ISRM) (AS/NZS ISO 31000:2009), information security training and awareness (ISTA) (ENISA, 2010b; Wilson et al., 1998), and information security incident response (ISIR) (ISO/IEC18044, 2006; Kibirkstis).

An example of a best-practice standard is the International Standard ISO 27000 series including, ISO/IED 27001:2013, *Information technology-Security techniques-Code of practice for information security controls*, which is widely accepted and adopted by organisations. Several industrial guidelines were also developed by the National Institute of Standards and Technology (NIST) (Swanson & Guttman, 1996) including the NIST Special Publication 800-14 *Generally accepted principals and practices for securing information technology systems*.

However, the guidance that existing industrial standards and best-practice guidelines provide to organisations on the range of ISMPs is limited for several reasons (Al-Ahmad & Mohammad, 2013; Nykänen & Hakuli, 2013; Siponen & Willison, 2009). These reasons can be divided into two main categories: the design and the development of the standards, and the organisations’ approach to adopting the standards (compliance).

There are several reasons related to the design and the development of the standards that affect the extent of guidance on ISMPs for organisations. First, existing standards and guidelines do not provide a clear definition of managerial practices nor do they maintain practice level recommendations. For example, the ISO/IEDC 27001 standard, which is considered by many practitioners to be the main reference for organisations when it comes to security practices, does not provide practice-level recommendations nor does it endeavour to distinguish between types of activities and controls (e.g. managerial-level and operational-level). Second, the standards are not based on empirical evidence and do not provide any justification for how the recommendations were identified (Siponen & Willison, 2009). Third, standards are too generic and recommended practices may not be applicable to every organisation (Siponen & Willison, 2009).

Another problem that also indicates the limited guidance the standards offer to organisations on ISMPs is that the standards tend to be used as a checklist of protective measures to be implemented to protect organisations. To comply with the standards, organisations should select controls that are applicable to the organisational context based on the risk assessment (Mesquida
However, the process of determining which controls are applicable is subject to the expert’s opinion. Shedden et al. (2010) performed in-depth case studies of three different organisations that claimed to be compliant with international information security standards. They found that it is unclear to organisations what they should do to meet compliance requirements. Organisations take three approaches to comply with the standards: (1) simplify the compliance process by finding ways to technically comply with the standards while expending minimal effort to do so, (2) implement as much as they can from the standards recommendations and (3) call a team from an external company to assist them to comply with the standard (Shedden et al. 2010). Ultimately, the choice of which controls to implement is left to the opinion of the experts and is therefore very subjective. Further, as Siponen and Willison (2009) point out, experts tend to check if these controls have been implemented rather than if they have been implemented correctly. Therefore, the standards tend to be used to look at the existence of the controls not the quality of the implementation (Siponen & Willison, 2009).

To sum up, this research argues that existing standards, especially ISO 27001, were not designed to provide practice-based guidance for organisations on the range of security practices in general, let alone the managerial practices. The standard provides guidance to organisations on the types of controls for different areas of information security management. However, there is no specific guidance on the practices that managers should carry out in order to implement those controls. Therefore, the existing professional literature does not provide coherent and sufficient guidance on the range of information security management practices that should be implemented in organisations.

2.3.2 Academic literature

A review of the academic literature on the ISM domain revealed that although considerable research has been done on the managerial aspects of information security, there has been no significant development in providing coherent and consistent guidance on the range of ISMPs that should be implemented in organisations.

The majority of the research effort in the ISM domain has focused on studying individual aspects of ISM and applying different theories. Theory building and theory testing research have implications for practice in organisations; however, the aim of this type of research is not to provide guidance on ISMPs. Examples of such studies include studies on policy compliance
(Bulgurcu, Cavusoglu, & Benbasat, 2010; Puhakainen & Siponen, 2010; Vance, Siponen, & Pahnila, 2012), security training approaches (Karjalainen & Siponen, 2011), improving the accuracy of risk assessment process (Shedden, Smith, Scheepers, & Ahmad, 2009; Webb, Ahmad, Maynard, & Shanks, 2016), stakeholders participation in the risk management process (Spears & Barki, 2010), and learning from incident response (Ahmad, Hadgkiss, & Ruighaver, 2012; Ahmad, Maynard, & Shanks, 2015). Although these types of studies have theoretical and practical contributions to the domain, they do not provide comprehensive guidance on the range of ISMPs.

The review also identified studies that have attempted to provide guidance for organisations on how to build their information security programs (Bayuk, 1997; Hong, Chi, Chao, & Tang, 2003; Oyelami & Ithnin, 2015; Qingxiong et al., 2008; Qingxiong, Schmidt, & Pearson, 2009; Tryfonas et al., 2001). This body of literature provides advice on security practices (strategic and operational-level activities) that should be implemented in organisations. In the following section, a review of some existing studies in the academic literature is presented.

### 2.3.3 Existing studies on ISMPs

There are several studies that aim to guide organisations to develop an effective information security program. This section discusses these studies and critically analyse them.

Information security is a multidimensional problem that is continually evolving and changing. Studies in the domain have evolved from approaching information security in a narrow technological perspective to managerial perspective and eventually the realisation of the importance to provide a holistic and comprehensive approach (Soomro et al., 2016).

A common characterisation of existing studies in the domain is the aim to provide guidance to organisations by the identification of activities that should constitute a security program. However, there is no consistent classification of managerial activities that the organisation should implement. One reason is that existing studies use different terms such as process, principles, practice, activity, theory to present their advice. Further, existing studies use different level of details and analysis in describing the activities that organisation should implement.

Therefore, by reviewing existing models and frameworks, it is difficult to determine what ISMPs that should be implemented because the lack of consistent classification and the use of different terminology and levels of granularity.
In terms of the type of security activities that are suggested to organisations, some of the existing studies mainly focus on technological activities. For example Keller, Powell, Horstmann, Predmore, and Crawford (2005) studied ISM in small organisations. The study identified nine commonly recommended “best practices”, particularly for small businesses. These practices include install and properly configure a firewall; update software; protect against viruses, worms, and trojans; implement a strong password policy; implement physical security measures to protect computer assets; implement company policy and training; connect remote users securely; lock down servers; and implement identity services (intrusion detection). The practices mentioned in the study range from purely technological practices with exception to implementation of policy and training.

While other studies provide suggestions that include managerial and technological activities. For example Tryfonas et al. (2001) identified security practices that should be integrated to information systems development process. These practices include managerial/ procedural practices such as establishment and use of the policy, compliance with security standards, copyright protection, risk analysis, and IS audit. The recommended practices also include technological such as applied cryptography solutions, network security and use of firewall, access control mechanism, software security practices, and intrusion detection techniques.

Also, existing studies in the domain differ in terms of the level of granularity and details when describing the suggested advice. Some studies provide descriptions of main processes and only lists activities they proposed as part of each processes (Bayuk, 1997; Oyelami & Ithnin, 2015; Qingxiong & Pearson, 2005). For example, Bayuk (1997) argued that an effective ISM process should consist of six sub-processes: policy, awareness, access, monitoring, compliance, and strategy. The author described each process and the activities undertaken as part of these processes. The policy process starts by identifying of what to secure, then proceeds through a series of prototype documents to produce a draft policy. Then the policy is approved and published. From this point, the process repeats itself as the policy is continuously updated.

Another example in the literature that attempts to provide guidance to organisations on the security management practices is proposed by Hong et al. (2003). Hong et al. (2003) defined information security as applying “any technical methods and managerial processes on information resources (hardware, software and data) in order to keep organisational assets and personal privacy protected” (p.243). The authors argue that there is a lack of guidance on ISM for organisation and that little empirical work has been conducted on the effectiveness of ISM
strategies and tools. Consequently, there is no consensus between academics and practitioners on what ISM involves. Hong et al. (2003) proposed an integrated system process of ISM which comprises five sub-processes: security policy, risk management, control and auditing, management system, and contingency. Table 2-1 summarises the ISM processes and the activities associated with each process.

<table>
<thead>
<tr>
<th>ISM theory</th>
<th>Managerial Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security policy</td>
<td>Security policy establishment</td>
</tr>
<tr>
<td></td>
<td>Security policy implementation</td>
</tr>
<tr>
<td></td>
<td>Security policy maintenance</td>
</tr>
<tr>
<td>Risk management</td>
<td>Risk assessment</td>
</tr>
<tr>
<td></td>
<td>Risk control</td>
</tr>
<tr>
<td></td>
<td>Review and modification</td>
</tr>
<tr>
<td>Control and auditing</td>
<td>Establish control systems</td>
</tr>
<tr>
<td></td>
<td>Implementing controls systems</td>
</tr>
<tr>
<td></td>
<td>Information auditing</td>
</tr>
<tr>
<td>Management system</td>
<td>Establish security policy</td>
</tr>
<tr>
<td></td>
<td>Define security scope</td>
</tr>
<tr>
<td></td>
<td>Risk management implementation</td>
</tr>
<tr>
<td>Contingency</td>
<td>Policy strategy</td>
</tr>
<tr>
<td></td>
<td>Risk management strategy</td>
</tr>
<tr>
<td></td>
<td>Control and auditing strategy</td>
</tr>
<tr>
<td></td>
<td>Management system strategy</td>
</tr>
</tbody>
</table>

While others (Cavalli et al., 2004; Diwakar & Naik, 2008; Keller et al., 2005) just list activities without providing classification and sufficient details on how these activities can be implemented in organisations. For example, Cavalli et al. (2004) provided a practical case of ISM in an Italian hospital. The authors described various practices and activities including developing a plan and selecting a team, evaluating CIA requirements, undertaking threat assessment to determine the probability and impact of a threat, carrying out a risk assessment and the implementing controls. These practices exist at different level of analysis. For example, the risk assessment includes the threat assessment and probability and impact of a threat, however the authors mentioned them as they are in the same level of analysis. It appears that the authors’ main focus was on how the hospital information security program is aligned with BS 7799.

Another example is the study conducted by Qingxiong et al. (2009) who argued that there is insufficient guidance for organisations on ISMPs. This situation is the result of the lack of consensus on how organisations manage their information security and the lack of holistic approaches to ISM in organisations. Qingxiong and Pearson (2005) conducted an empirical
validation of the international security management standard ISO 17799 (now known as ISO 27001) through a survey of information security professionals. The validated security practices can be used by organisations as checklists or guidelines to manage their information security program.

Another study was carried out by Qingxiong et al. (2008) to develop a comprehensive framework for ISMPs in organisations. Qingxiong et al. (2008) develop a framework for ISM based on academic and professional literatures, and then refined the proposed framework via survey data from information security experts. These studies did not provide enough details nor consistent classifications of the proposed practices.

The analysis of existing studies revealed that there is a common way of presenting activities which has been adopted by several authors (Bayuk, 1997; Chaudhry et al., 2012; Guzman, Galvez, Stanton, & Stam, 2010; Hong et al., 2003). These studies present main categories/themes of ISMP that are referred to in different terminologies (processes, theory, principles, practices, components). Each of the main categories consists of a number of activities.

Further, from the analyses (main categories in Section 3.4 and Section 4.2 as well as activities within each category – see Table 2-2), it was clear that information security management practices can be classified into four main common categories. This research refers to the four main categories as ISMP areas. These areas are: risk management, policy management, information security training and awareness (ISTA) and incident response management.

Table 2-2, almost all existing information security management studies mention information security policy as one of the main areas of ISM (Qingxiong et al., 2008; Savola et al., 2006). For example, both Hong et al. (2003) and Oyelami and Ithnin (2015) report policy as a major ISM area. Research describes components of the security policy and report several activities related to security policy. These activities include: analyse information security requirements, form and draft policy, implement the policy and maintain this policy (Hong et al., 2003; Oyelami & Ithnin, 2015). Similarly, Bayuk (1997) includes policy as one of the main processes of ISM. The policy process starts by identifying what to secure, then proceeds through a series of prototype documents to produce a draft policy. Then the policy is approved and published. From this point, the process repeats itself as the policy is continuously updated.
Table 2-2 Analysis of common ISMP areas in existing ISM literature

<table>
<thead>
<tr>
<th>ISMPs studies</th>
<th>Risk management</th>
<th>Policy management</th>
<th>Security training and awareness</th>
<th>Incident response management</th>
<th>Audit and compliance</th>
<th>Top management support</th>
<th>Access control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bayuk (1997)</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Tryfonas et al. (2001)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hong et al. (2003)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cavalli et al. (2004)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diwakar and Naik (2008)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guzman et al. (2010)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zuccato (2007)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chaudhry et al. (2012)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Lim et al. (2012)</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qingxiong and Pearson (2005)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qingxiong et al. (2008)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qingxiong et al. (2009)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tashi and Ghernouti-Hélie (2009)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kwon and Johnson (2013)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oyelami and Ithnin (2015)</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The second most commonly researched area of ISM is risk management. The risk management area is very important to identify and manage information security risks and identify the type of security controls that the organisation should implement to protect information resources (Bayuk, 1997; Cavalli et al., 2004; Cavusoglu, Cavusoglu, & Raghunathan, 2004; Hong et al., 2003).
2003; Oyelami & Ithnin, 2015; Qingxiong et al., 2008; Tryfonas et al., 2001). According to Hong et al. (2003) the risk management process consists of three main activities: risk assessment, risk control, review and modification.

Incident response management includes the implementation of procedures and other controls capability of swift detection and response to security incidents (Cavalli et al., 2004). Incident response is usually mentioned as part of the ‘Do’ phase of the information security lifecycle (Cavalli et al., 2004; Qingxiong et al., 2008; Qingxiong et al., 2009).

Other non-technological areas covered in existing literature include audit and compliance, top management support, access controls. This thesis argues that practices and activities within these areas do not fall under information security management practices. For example, audit and compliance activities that reported in several studies are conducted as the review process that organisations implement to ensure ISMP is implemented to meet compliance and regulatory requirements. While top management support represents the security effort to gain management commitment and support of information security (Lim et al., 2012). The other two common areas are ‘access controls’ and ‘monitor and review process’ (Bayuk, 1997; Chaudhry et al., 2012; Oyelami & Ithnin, 2015). These two areas usually refer to the implementation of technological controls to limit unauthorised access and monitor the organisation information systems. Therefore, these areas are not considered as part of the management process of information security program.

2.3.4 Analysis of the existing models and frameworks
A review of existing studies in ISM was undertaken to guide organisations in developing an effective information security program. Although considerable effort has been expended, existing studies do not provide a consistent and coherent view of ISMPs. This is because the aim of this body of literature is not to develop guidance on managerial practices and even though models and frameworks proposed cover certain aspects of ISMPs with various levels of granularity, they do not provide a clear definition of the term ‘ISMP’ and what it involves.

Overall the lack of consensus on what ISM involves and the lack of focus on ISMPs has affected the level of guidance that existing models and frameworks can provide to organisations as the authors have not been able to build on a consistent, coherent explanation of what activity should be implemented and how to implement it. Organisations have no standardized and formal checklist to benchmark or audit their existing ISMPs or assess their level of maturity.
2.4 The identification of the research problem

The review of literature on ISMPs found three deficiencies that profoundly affect the level of protective guidance afforded to organisations. These deficiencies are: (1) poor conceptualisation of ISMPs; (2) the lack of comprehensive guidance on ISMPs; and (3) the lack of empirical work in the area and more specifically in the practices. The consequences of inadequate managerial guidance on information security are significant for the modern organisation, given the significant exposure to security threats. Table 2-3 maps the existing frameworks and models in ISM with the three identified deficiencies.

Table 2-3 Summary of the existing ISM frameworks and models in relation to the three identified deficiencies.

<table>
<thead>
<tr>
<th>ISMPs studies</th>
<th>Deficiency 1</th>
<th>Deficiency 2</th>
<th>Deficiency 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bayuk (1997)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Tryfonas et al. (2001)</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Hong et al. (2003)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Cavalli et al. (2004)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Diwakar and Naik (2008)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Guzman et al. (2010)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zuccato (2007)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Chaudhry et al. (2012)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Lim et al. (2012)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Qingxiong and Pearson (2005)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Qingxiong et al. (2008)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Qingxiong et al. (2009)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Kwon and Johnson (2013)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Oyelami and Ithnin (2015)</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

In the remainder of this section the abovementioned deficiencies are explained in more detail.

2.4.1 Deficiency 1: Poor conceptualisation around ISMPs

One of the earliest studies in the literature suggests that the managerial aspects of information security are “largely diffuse and unorganised” (Madnick, 1978, p.61). This research argues that it is still the case today. In the same vein, Choobineh et al. (2007) stated that:
information security management is a relatively immature discipline and that it requires additional academic study. We believe that there is a growing need for research to verify/confirm the management challenges, discover current management deficiencies, identify best practices, devise methodologies, and specify requirements for the management of information security. (p.959)

A key indication of the immaturity in the discourse around (ISM) is a lack of a consensus on terminology around management practice that used across the literature. For example, the terms managerial control (Whitman & Mattord, 2011), formal and informal controls (Dhillon, 2007a), practice (Lim et al., 2012), and process (Purser, 2004a) have been used to describe information security management activity. These terms are frequently not defined and are used by different authors to mean different things. For example, some authors (Guzman et al., 2010) use the term ‘security practices’ to refer to technological controls such as firewalls, while others Lim et al. (2012) consider organisational factors such as top management support and budget allocation as security practices.

The poor conceptualisation has led to an unclear definition of the boundaries of the ISMPs in the domain. Therefore, there is a lack of systematic classification of security practices (Hong et al., 2003; Tryfonas et al., 2001). There are inconsistencies in both the academic and professional literatures when referring to ISMPs, with the range of ISMPs varying with different researchers and institutions (see Section2.3.3). For example, Tudor (2006) stated that there are six processes of ISM which include: security organisations, security policy and procedures, security baseline and risk assessment, security awareness and training, compliance, and computer incidents, while the ISO 27002 provides a different scope of ISM (Hong et al., 2003).

A further indication of the immaturity in the discourse is the lack of agreement on the levels of granularity in management activities. For example, Choobineh et al. (2007) use ‘strategic’ and ‘operational’ levels of granularity while Purser (2004b) uses ‘strategic’ and ‘tactical’ levels. Additionally, information security management industry standards contribute to the confusion surrounding levels of granularity and usage of terminology. For instance, the ISO27002:2006 standard for the code of practice of information security management is organised into eleven different sections (with no justification for this method of classification), each consisting of a range of recommendations, and with no distinction between types of activities and controls (e.g. managerial-level and technological -level). Qingxiong and Pearson (2005) cited the need for more study on the implementation of information security initiatives needs more study because information security practices can be defined at different level and have different implementation priority.
Since the early characterisation of (Madnick, 1978), there has been no significant increase in research activity addressing the need to develop a coherent and comprehensive view of ISMPs. In essence, this points to the lack of a theoretical framework and conceptualisation of ISM implementation as discussed by Choobineh et al. (2007).

The discipline is unable to progress and develop as a research discipline if researchers cannot even agree on basic terminology. Therefore, from a discipline point of view it is fragmented, it is not cumulative in that authors do not build on each other’s contributions, there is no consensus on foundational principles and concepts and there is no coherent view of practices. From the above discussion, this thesis argues that there is a need to identify, classify and understand the management practices of information security.

This thesis sees ISM as a process consisting of a number of practices. The term ISMP is used exclusively for managerial activities and does not therefore include operational activities.

**2.4.2 Deficiency 2: The lack of comprehensive guidance on ISMPs for organisations**

Several researchers have cited the lack of comprehensive work in the ISM area and the need for a holistic and comprehensive approach (Lim et al., 2012; Soomro et al., 2016; Zafar & Clark, 2009; Zafar et al., 2014). For example, Zafar and Clark (2009) and Zafar et al. (2014) stated that information security is widely regarded as a field that lacks comprehensive research. Lim et al. (2012) reinforce this point, stating that although a number of studies do cover individual security ISMPs, none provide a comprehensive overview of these practices. Ma et al. Qingxiong et al. (2008) also recognise the need for a comprehensive list of ISMPs and attempts to address this need. However, their ISMP framework has a number of issues. First, the framework does not distinguish between managerial and technological practices. For example, one of the ISMPs in the proposed framework is installing virus protection software, which is clearly not a management practice. Second, the framework does not distinguish between various levels of granularity (e.g., strategic, tactical and operational) of management-level activity. Finally, the ISMPs in their framework have been taken exclusively from the ISO 17799 standard and have not considered either the academic or professional literature.

Hong et al. (2003) argued that there is a lack of coherent and comprehensive understanding information security management process. They proposed an integrated process of ISM based on their review of the literature. The integrated process includes several sub-processes: security
policy, risk management, control and auditing, management system and contingency. Each sub-process has different managerial activities. The proposed ISM process has several issues. First it is not based on a comprehensive review of the literature. Second, it does not provide a detailed description of the managerial activities of each area. For example, the information security policy process includes three high-level managerial activities namely: security policy establishment, security policy implementation and security policy maintenance with no further guidance on how these activities are conducted in organisations. Lastly, the proposed process is not backed by empirical data. These issues undermine the usefulness of the proposed theory in providing sufficient guidance to organisations.

Several researchers highlighted the importance of a comprehensive and holistic approach for information security management (Eloff & Eloff, 2003; Soomro et al., 2016; Swanson & Guttman, 1996). For example, Dhillon (2007a) argues that an effective security management program should integrate different information security processes, such as information security risk management, educating personnel in information security awareness, and establishing and executing ISPs.

Additionally, NIST SP 800-14 emphasised the importance of a comprehensive approach that considers a variety of areas within the ISM domain. They pointed out that, “to work effectively, security controls often depend upon the proper functioning of other controls” (Swanson & Guttman, 1996, p.9). Therefore, a comprehensive approach is required to achieve a high level of synergy between different areas of ISMPs.

However, without a firm understanding of the interdependencies of security practices, they can undermine one another. For example, without accurately identifying information security risks through a formal risk assessment process, the quality of the developed ISP will be affected, as it depends on the accurate identification of the information security risks. Another example for the interdependencies between ISM areas is that between ISP and the ISTA program. ISTA program is essential to communicate policy and raise the awareness of the organisation’s employees of the policy. If the organisation has an effective communication of ISP through the ISTA program, then it is more likely employees will comply with the organisation’s policy. Swanson and Guttman (1996) state that “Many other important interdependencies exist that are often unique to the organisation or system environment. Managers should recognize how computer security relates to other areas of systems and organisational management” (p.9).
Therefore, it is important to provide comprehensive guidance to organisations on the managerial practices of information security and how they can be implemented in a holistic and collective manner to ensure high level integration and synergy between ISMPs and hence, an effective management of information security in organisations.

2.4.3 Deficiency 3: the lack of empirical work in the ISM area more specifically into the managerial practices

Much of the existing work on ISMPS has been based on conceptual analysis and the opinion of industry professionals, with very little empirical evidence presented to justify the recommended practices (Ezingeard & Bowen-Schrire, 2007; Qingxiong et al., 2008; Siponen, 2005; Tryfonas et al., 2001).

Dhillon et al. (2007) and Dhillon and Backhouse (2001) argue that the lack of empirical work has result in limited understanding of what ISM involves, which led to insufficient guidance on the ISMPs that the organisations should implement. They stated that

*There is limited understanding of various dimensions that result in information systems security problems. There is very little empirical research that has investigated various aspects of information systems security, in particular the nature and scope of its dimensions. There is also a limited understanding of how organisations manage the various information systems security dimensions and what potential problems there might be. As a consequence, there is a clear need to identify and establish mechanisms that would be required to successfully manage information systems security.* (p.1)

In the past decade, more empirical research has been conducted in various areas on ISM. However, much of the empirical research has been focused on using theories and developing frameworks to:

1. investigate Information security policy quality (Ruighaver, Maynard, & Warren, 2010), compliance, user behaviour, and establishing an information security culture (Balozian, Leidner, & Warkentin, 2017; Inho, Daejin, Taeha, & Sanghyun, 2017; Lim, Maynard, Ahmad, & Chang, 2015),
2. assess the implementation of risk management standards in organisation (Shedden, Ruighaver, & Ahmad, 2006) and improve the accuracy of risk assessment process (Webb, Ahmad, Maynard, & Shanks, 2014; Webb et al., 2016),
3. study the effect of ISTA on the overall information security of organisations (Öğütçü, Testik, & Chouseinoglou, 2016)
4. planning for security incidents (Line, Tondel, & Jaatun, 2014), and learning from responding to incidents to improve the overall security management process (Ahmad, Maynard, et al., 2015).

Although such research has provided recommendations and suggestions on those specific aspects of ISM area, there has been little empirical research conducted on synthesising ISMPs to provide sufficient and coherent guidance for organisations (Qingxiong et al., 2008). Similarly, Tryfonas et al. (2001) cite concerns about the lack of proven scientific approach for ISM and consider this issue as one of the main issues in the domain. Ezingeard and Bowen-Schrire (2007) also call for more interpretive studies to provide a better understanding of the ISM process.

Additionally, organisations rely on ISM industry standards to guide them in managing their information security programs. However, as previously mentioned, these standards are not based on empirical evidence and do not provide any justification for how the recommendations were identified (Siponen & Willison, 2009). Therefore, this research project aims to develop a coherent, comprehensive and empirically tested framework of ISMPs.

2.5 Summary
This chapter provided an overview of information security. It has also discussed the importance of ISMPs. This chapter also presented a review of both academic and professional literatures, which includes critical analysis of the existing models and frameworks that were developed to assist organisations to develop an effective information security programs. The review of the existing ISM literature regarding the provision of ISMPs guidance has led to the identification of three deficiencies. This research project aims to develop comprehensive, coherent and empirically tested guidance for organisations on the range of ISMPs by addressing the identified deficiencies. The next chapter will describe the research design for this research.
Chapter 3 RESEARCH DESIGN

3.1 Introduction
This chapter explains the research design used in this project and justifies the theoretical perspective adopted. The selection of an appropriate research paradigm and research design is an important step for enabling reliable knowledge. An overview of the research design is outlined, including the three main phases conducted as part of this research. This chapter also provides a detailed description of the comprehensive review undertaken to develop the research framework, and data collection tool (semi-structured interview) and the methods for data analysis.

3.2 Research characteristics of this study
This section provides an overview of the research paradigm and research methods used in the information systems (IS) domain. It also describes and justifies the research methods that have been adopted in this research project.

3.2.1 Research paradigm
The research paradigm refers to the theoretical belief and perspective that the research holds, which guides the researcher’s view of the world. It also dictates the way researchers conduct research and the conclusions they make. There are three main philosophical paradigms in information systems research: positivist, interpretivist, and critical realism (Orlikowski and Broudi, 1991). Positivist and interpretivist paradigms are considered to be more common than critical realism in IS research.

According to Orlikowski and Broudi (1991), in the interpretivist paradigm “people create and associate their own subjective and intersubjective meanings as they interact with the world around them” (p. 5). Interpretivists hold the belief that an in-depth understanding of the research phenomenon cannot be achieved in isolation from how they are perceived by people. Therefore, direct engagement with the people (research subjects) is very important for understanding people’s views and the surrounding environment (Dwivedi & Kuljis, 2008). Interpretivist
research is usually aimed at making sense of the research phenomenon and builds theory based on the research findings (Creswell, 2013).

The choice of philosophical paradigm depends on the nature and purpose of the research, and the researcher’s orientation. Darke, Shanks, and Broadbent (1998) and Orlikowski and Baroudi (1991) have defined key points that should be considered by the researcher to determine if the interpretivist paradigm is suitable for a particular research project: the researcher should acknowledge that reality is subjective and the research is not “value free”, the research should not aim to discover repeatable patterns in the investigated phenomenon, and the research intends to provide an in-depth understanding of the phenomenon.

In this research project, the interpretivist paradigm is adopted and considered to be the most appropriate paradigm as the researcher aims to provide an in-depth understanding of how ISM is practiced in organisations. For this purpose, the researcher should engage with people who are involved in implementing ISMPs in organisations. Input from research participants (i.e. information security managers and information security consultants) were the primary source of information for informing and analysing the research phenomena. The input was obtained by conducting qualitative interviews which provided rich data and an in-depth understanding.

3.2.2 Nature of this research

Neuman (2013) classified research into three types: descriptive, explanatory, and exploratory. Descriptive research aims to collect a wide range of data about an existing situation or issue (Creswell, 2013). Explanatory research aims to explain why a particular thing happens, and it is used when the description of the issues already exists (Neuman, 2013). Exploratory research provides a better understanding of a phenomenon (Yin, 2003). It is typically used in theory building research (Shanks, Arnott, & Rouse, 1993). This research is exploratory, as it aims to better understand and identify the managerial practices of information security.

3.2.3 The role of information systems theories

Theories play an important role in research since they interconnect ideas around the knowledge of the social world (Neuman, 2006). In particular, theories used in organisational studies provide a system of interconnected concepts and ideas that organise knowledge about how and why people behave in organisations. Theories are abstract entities with objectives to provide descriptions and explanations (Gregor, 2006; Miner, 2015), and also able to predict what will happen in the future (Gregor, 2006). According to Gregor (2006), IS researchers use a theory
(or theories) for analysing, explaining, predicting and designing, to make sense of people’s use of technologies.

From a theoretical perspective, this research project falls under Gregor’s (2006) Type I: Theory of Analysing and Type II: Theory Explaining. Gregor (2006) describes analytic theory as the most basic type of theory where the objective is to “…describe or classify specific dimensions or characteristics of individuals, groups, situations, or events by summarizing the commonalities found in discrete observations” (p.623). Analytic theory seeks to answer, the “what is” research question and the theory of explaining seeks to answer the “how” research questions. Theory of explaining provides explanations for how and why things happened in some particular real-world situation. The research approaches that can be used to develop the theory of explaining include case studies, surveys adopting an interpretivist paradigm (Gregor, 2006).

This research project seeks to answer the “How” and “what” questions by explaining how ISM is practiced and by identifying and classifying ISM-type activities. Thus, in terms of information systems theories, the analytic theory and explaining theory are the most appropriate theories to describe this research project.

3.2.3.1 The systems theory application in this research

The systems theory has had a significant effect on management science and understanding organisations (Johnson, Kast, & Rosenzweig, 1964; Kast & Rosenzweig, 1972). A system is a collection of parts unified to accomplish an overall goal. If one part of the system is removed, the nature of the system is also changed. A system can be looked at as having inputs (e.g., resources such as raw materials, money, technologies, and people), processes (e.g., planning, organising, motivating, and controlling), outputs (products or services) and outcomes (e.g., enhanced quality of life or productivity for customers/clients, productivity). Systems share feedback among each of these four aspects of the system (Checkland, 1994).

The effect of systems theory in management is that it helps managers to look at the organisation more broadly. It has enabled managers to interpret patterns and events in the workplace, that is by enabling managers to recognise the various parts of the organisation, and, in particular, the interrelations of the parts (Chikere & Nwoka, 2015; Luoma, Hämäläinen, & Saarinen, 2007).

The systems concept calls for integration of activities related to particular projects or programs into a separate organisational system (Arnold & Wade, 2015; Reynolds & Holwell, 2010). This
approach currently is being implemented in some of the more advanced-technology industries (Laszlo & Krippner, 1998). This concept of the organisation can be used by practicing managers to integrate the various ongoing activities into a meaningful total system (Reynolds & Holwell, 2010).

Managers are needed to convert disorganised resources of men, machines, and money into a useful, effective enterprise. Essentially, management is the process whereby these unrelated resources are integrated into a total system for objective accomplishment (Checkland, 1994; Laszlo & Krippner, 1998). The systems concept does not guarantee managerial success. The basic functions are still planning, organisation, control, and communication. Each of these activities can be carried out with or without emphasis on systems concepts (Checkland, 1994). Johnson et al. (1964) stated that the activities themselves can be better accomplished using systems concepts. Furthermore, there can be a definite change in emphasis for the entire managerial process if the functions are performed in light of the system as a whole and not as separate entities.

Since this research seeks to identify the range of ISMPs that are implemented in organisations to protect their information resources, the researcher searched in the general management literature and found that systems theory was the most suitable theoretical model for this study. This theory was chosen because it aims to provide a systematic, theoretical framework for describing relationships between elements of systems (von Bertalanffy, 1968). The systems theory can also identify existing similarities in the theoretical construction of various disciplines; therefore, models can be developed that have applicability to many fields of study (Chikere & Nwoka, 2015).

The systems theory is used to assist the researcher in conceptualising ISMPs and constructing a holistic view of the ISM process in organisations. The systems theory guided the researcher to develop a broad understanding of the phenomenon of ISMPs, which has led to further investigation and review of the literature around what ISMPs the organisations can implement. The systems theory plays an important role in this research. The systems theory has been applied in this research at two different levels.

First the systems theory was applied to the initial stage of this research where the research was trying to establish a comprehensive understanding of the information security management as subsystem of the organisation. The systems theory at this stage enabled the researcher to understand the phenomenon under investigation (ISM) and its context within the organisation.
Therefore, the systems theory played a role in focusing the researcher’s attention on the process aspect, which lead to synthesising the knowledge in the literature around ISMPs and developing a theoretical framework as an outcome of the research project. This research proposes a framework that provides sufficient and coherent guidance to organisations for managing their information security program.

Second, the systems theory was applied to guide data collection and analysis to identify relationships and interdependencies between information security management practices. As explained in Section 2.4.2, while much research has been focused on the analysis of knowledge around individual ISM areas, there has been increasing interest in developing larger frames of reference for synthesising the results of such research. Thus, significant attention has been focused on overall systems (ISM) as frames of reference for analytical work in various areas. The systems theory was applied recursively regarding ISM as a system and aiming to determine subsystems that constitute the ISM and the relationships between these subsystems.

Managers have often focused attention on particular functions in specialised areas, and they may therefore, lose sight of the overall objectives of the business and the role of their particular business in even larger systems (Checkland, 1994; Luoma et al., 2007). These individuals can carry out their responsibilities better if they are aware of the ‘big picture’. It is the familiar problem of not being able to see the forest for the trees. The systems theory approach provides a better picture of the network of subsystems and interrelated parts that go together to form a complex whole. This approach provides a useful way to conceptualise ISMPs and assist in drawing the boundaries between different related concepts.

3.2.4 Research methods

Due to the interpretivist, theory building and explorative nature of this study, the research project follows a qualitative, rather than a quantitative approach to answer the research questions. The qualitative approach enables the researcher to gain an in depth understanding by providing the opportunity to investigate the research phenomenon and the context. Within this approach, the findings are based on a specific studied context in which the research questions are raised. From an interpretivist philosophical perspective, the qualitative approach is the most appropriate as it facilities a better understanding of the perceptions, beliefs and attitudes of the participants that affect their behaviours (Myers & Newman, 2007).
By using a qualitative approach, the collected data comes from organisations through interviews, document analysis, and observations whereas data analysis uses qualitative analysis techniques. This approach provides the opportunity to investigate organisational behaviours and practices deeply and in rich detail. The problem with this approach is that the findings are based on a specific studied context and cannot be easily generalised. A qualitative approach has a significant value because it allows researchers to investigate the context in which the research questions are raised. It furthermore provides a better understanding of the perceptions, beliefs and attitudes of the participants that affect their behaviours (Myers & Newman, 2007).

The researcher followed the qualitative research methodology because of the need to understand the phenomenon (ISMPs) from the participants (information security managers) in a natural setting. Additionally, the qualitative approach is flexible, as the design is suited to the demands of research situation, and the data collection and analysis instruments are not standard (Lee, Mitchell, & Sablynski, 1999). While a quantitative approach, for example a survey, can be used to investigate information security management practices in organisations, it cannot capture from the participants’ perspectives how ISMPs are implemented and why a particular approach was taken to the implementation. Studying ISMPs using the qualitative approach will enable more understanding of the phenomena. Therefore, developing a good understanding of the research phenomena will allow quantitative approach to be used in the future to provide more generalisation of the research findings.

### 3.3 Research Design

The research design of this project consists of three main phases: the contextual study, the conceptual study and the empirical study (see Figure 3-1).

![Figure 3-1 Summary of the Research Design](image)
3.3.1 Phase 1: Contextual study

The contextual study involves conducting a conventional literature review to develop an understanding of the ISM area and identify gaps and limitations in the area regarding managerial practices. It has been concluded from the review, which was presented in Chapter 2 that there is a lack of understanding around the managerial practices of information security. The outcome of this phase was to define the research context, namely the research problem, research gap, significant, research questions and research design.

3.3.2 Phase 2: Conceptual study

In the second phase, in order to find a theory that could be used as a lens to guide the investigation of the phenomena, the researcher has examined several theories from different disciplines (Information System, Management, and Criminology). Unfortunately, the researcher could not find a theory that was suitable for the nature of this research project. Therefore, a synthesis of the body of knowledge on ISM was considered to be the most appropriate way to achieve the objectives of this research. The relevant literature on ISM was comprehensively reviewed based on (Okoli & Schabram, 2010)’s approach. The grounded theory analysis process was followed to analyse the literature (Wolfswinkel et al., 2013). The findings of this phase have led to a research framework for ISMPs that can be implemented by organisations to safeguard their information assets. The review and analysis of the literature was conducted in two rounds. The first-round of review used a general search terms to identify ISMPs in the literature and resulted in the identification of four ISMP areas. More details on how the comprehensive literature review was conducted is presented in Section 3.4 and Section 4.2.

The second step focused on the analysis of the literature of each of ISMP areas. This resulted in the development of an ISMP framework for each area in chapter 5-8. For more details about the second round of review and analysis see Section 0

3.3.3 Phase 3: Empirical study

This phase aims to validate and refine the proposed conceptual framework by conducting interviews with security experts and leaders in the industry. To obtain high-quality data, participants with expertise in the field were selected. This phase involves two sequential rounds of data collection: (1) semi-structured interviews to refine the ISMP framework of each areas, and (2) follow up interviews for final validation of the framework.
In the first round of data collection, thirty-four interviews with security experts (security managers, security consultants, and Chief Information Security Officer) were conducted. The participants were asked to describe what they do as part of their responsibilities with regard to one or two ISMP areas (policy management, risk management, ISTA management and incident response management) (see Section 3.5). In the data analysis, standard coding techniques (open, axial and selective coding) were used. New themes were mapped to refine the model (see Section 3.6).

In the second round of the data collection, the refined framework of the areas was sent to the participants to provide comments and feedback about the practices and key activities. The analysis and results of this was added to each chapter in final validation section.

3.4 The Conceptual Study
The conceptual study encompasses a literature analysis and knowledge synthesis of the literature related to ISMPs. The comprehensive literature review method was adopted to synthesise the existing body of knowledge in the ISM area, focusing on managerial practices. The comprehensive review and synthesis of the literature resulted in the development of the preliminary framework of ISMPs.

A search protocol was prepared which includes the research questions for the investigation. It also includes a plan for how the review process should proceed. The plan specifies the sources of ISM literature, criteria for screening, when to stop the search, etc.

In order to improve the reliability and consistency of the search and analysis process, the student analysed several articles and discussed the results of the analysis in the supervisory meeting. The discussion was focused on how the search and analysis process were conducted. This process provided inter-rater reliability and ensured that the researcher had a good understanding of the area and the ability to identify practices using ISMPs definition.

Two rounds of comprehensive search in the academic and professional literatures were carried out in this project. The first search was in the general ISM literature and the second search was directed to literature in individual ISMP areas that had been identified form the analysis of the first round of review. The two rounds of the literature search are described in detailed in Section 4.3.
3.4.1 Literature analysis and knowledge synthesis

This aim of the literature analysis and knowledge synthesis is to develop a robust and a comprehensive understanding of managerial practices relating to information security. Knowledge synthesis can assist in addressing the inconsistencies within a particular research area (Kastner et al., 2012); therefore, it has been used in this research project to clear the confusion about the phenomena under investigation, in terms of identifying ISMPs and setting the boundaries around them.

As outlined in Section 3.2.2, this project is exploratory in nature and theory building in research. Therefore, the grounded theory analysis technique was utilised to analyse the literature in order to develop an ISMP framework. Grounded theory is defined as “a general methodology for developing theory that is grounded in data systematically gathered and analysed” (Strauss & Corbin, 1994, p 273). The inductive approach of grounded theory enables the researcher to analyse the literature, focusing on theory building. Although the main purpose of grounded theory is to develop theory based on primary data collected by the researcher, it can be also used to synthesise literature-based secondary data (Wolfswinkel et al., 2013). Several researchers have argued that utilising grounded theory in literature reviews is a systematic and rigorous method that leads to a comprehensive and theoretically relevant analysis of a given topic (Wolfswinkel et al., 2013).

The researcher engaged in the coding process (open, axial and selective) and followed Wolfswinkel et al. (2013)’s guide for using grounded theory as a review method. The following steps were applied to analyse the literature:

i. After the set of articles to be reviewed was selected and retrieved, a random selection of the set was chosen and reviewed. All findings and insights that pertained to the research question are highlighted. The highlighted words, sentences, and paragraphs represented relevant ‘excerpts’.

ii. **Open coding:** in this step, the researcher re-read the excerpts and grouped excerpts that revolve around similar topics into concepts. Those mutually exclusive concepts must be either well-defined in the literature or can be well-defined. The open coding process resulted in identifying managerial activities of information security.

iii. **Axial coding:** The managerial activities that were related to each other were grouped into one managerial practice. Eventually there were several practices, each practice consists of a number of activities.
iv. **Selective coding:** in this step, the main practices are then refined, and interrelated practices were grouped into one main category which is practice area.

The coding process resulted in the identification of four main practice areas. Each practice area consisted of several managerial practices and each managerial practice consisted of several managerial activities. During the coding process, the researchers engaged in ‘comparative analysis’, which entails continuous comparison, linking, and relating of the identified practice areas, practices and activities (Wolfswinkel et al., 2013). They were also extensively discussed amongst the researcher and his supervisory team.

As the initial set of publications were reviewed, the researcher conducted a second-round literature review which was guided by the analysis of the first round. A comprehensive search was conducted on several databases of managerial practices and activities within each practice area (see Section 4.3.2). More details on the search and analysis are presented in the chapters 5-8 that discuss practices within each practice area.

### 3.5 Empirical study

The empirical study was conducted to validate and refine the proposed conceptual framework. It involved conducting semi-structured interviews with security experts and leaders in the industry and analysing the obtained data.

#### 3.5.1 Interviews

In this research project, semi-structured interviews with ISMP areas experts were the primary source of data collection that were used to validate the preliminary framework that was developed from the conceptual phase. It is regarded as the most common qualitative data collection technique (Ezzy, 2013).

There are three types of interview structure: unstructured, semi-structured, and structured. The difference between these three types is the way the interview is conducted, and more specifically, the type of questions presented. In unstructured interviews, no predetermined questions are prepared, and the questions will depend on the responses of the participant. Semi-structured interviews involve presenting primary questions and then managing the process by asking questions based on the subject’s answers to elicit more rich information. In structured interviews, each participant is asked the same pre-planned questions, once the participant answers a question the researcher asks the next question.
The semi-structured interview was selected as it enables the researcher to ask questions based on the research framework and allows further questions to ask for more clarification and to gain in-depth information based on their responses.

3.5.1.1 Interview protocol

The first step in preparing for the interviews was developing the interview questions. The interview questions were developed based on the preliminary framework of ISMPs. The interviews were divided into three main parts:

1) **Basic information section**: The purpose was to capture general information about the participant’s role, experience, and role and responsibilities regarding ISMPs; the organisation size, and the industry sector in which the organisation operates.

2) **ISMPs section**: This section was the main section of the interview protocol in which the participants were asked to describe the practices and activities they undertake as part of the management process of one ISMP area (risk management, policy management, ISTA, incident response) based on their role, and prior and current experience in the ISM domain. The purpose of this part was to identify ISMPs in organisation and to understand how they were implemented in different organisational contexts.

3) **Communication with stakeholder section**: the purpose of this section was to understand the role of stakeholders and identify strategies to communicate effectively with relevant stakeholders in order to increase their participation in ISM process.

Five interviews as a pilot study, were conducted to test and refine the interview protocol. The questions were also refined as the researcher leaned throughout the interview process.

3.5.1.2 Selection and recruitment process of the participants

The selection of the participants was based on their experience in the ISM domain and in one or two areas of ISMPs in particular that were identified in the conceptual study (information security policy, ISTA, etc).

In terms of the recruitment process, participants were identified through personal contacts of the researcher, snowballing, organisations’ websites, and LinkedIn. The researcher was also able to identify and invite potential participants by attending workshops and development sessions organised by security groups such as the Australian Information Security Association.
(AISA), which enabled the researcher to talk about his research project with security professionals and invite them to participate.

In preparation for the data collection phase a research ethics application was submitted to the University of Melbourne, Melbourne School of Engineering Human Ethics Advisory Group (ID 1443194.1). It was essential to obtain ethics approval to ensure that the ethics requirements of the research were satisfied, and the privacy of the participants was guaranteed. A plain language statement and consent form were also developed as part of the research ethics application. They were sent to the participants to provide them with in-depth information about the aims and objectives of the research, how the privacy of their personal and organisational information was to be assured, the importance of their participation, and their right to withdraw their participation at any time without penalty (see Appendix A).

After identifying the targeted participants, invitation emails were sent that contained an outline of the research project (research problem, approach for addressing the problem, and expected contributions). In addition, experts were provided with a brief description of the role the researcher intended them to play in the research. Once a positive response was received from an expert, he/she was contacted again to arrange a suitable time and location to conduct the interview. For those who did not respond to the invitation email, the researcher sent another email to remind them.

A total of 34 interviews were conducted with Melbourne-based information security management experts (see Table 3-1), including information security managers, chief information security officers, information security policy managers, information security awareness managers and information security consultants. There is no consensus on the acceptable number of interviews required for a qualitative research project as it depends on the research phenomena and how adequate the information that is provided by the participants. However, Bertaux (1981) argued that “fifteen is the smallest acceptable sample for qualitative research” (p.35).
<table>
<thead>
<tr>
<th>ID</th>
<th>Industry</th>
<th>Position</th>
<th>Experience</th>
<th>ISM areas/Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1_Mng_Policy</td>
<td>Financial (Banking)</td>
<td>Security Policy Manager</td>
<td>16+ Years</td>
<td>Policy &amp; IOL</td>
</tr>
<tr>
<td>P2_Cons_Policy</td>
<td>Information Technology and Services</td>
<td>Security Consultant</td>
<td>10+ Years</td>
<td>Policy &amp; IOL</td>
</tr>
<tr>
<td>P3_Cons_Policy</td>
<td>IT company</td>
<td>Security Consultant</td>
<td>10+ Years</td>
<td>Policy &amp; IOL</td>
</tr>
<tr>
<td>P4_Mng_Policy</td>
<td>Telecommunication</td>
<td>Security Manager</td>
<td>10+ Years</td>
<td>Policy &amp; IOL</td>
</tr>
<tr>
<td>P5_Cons_Policy</td>
<td>Consultancy</td>
<td>Security Consultant</td>
<td>7+ Years</td>
<td>Policy &amp; IOL</td>
</tr>
<tr>
<td>P6_Mng_Risk</td>
<td>Telecommunication</td>
<td>Security Manager</td>
<td>15+ Years</td>
<td>Risk &amp; IOL</td>
</tr>
<tr>
<td>P7_Mng_Risk</td>
<td>Consultancy</td>
<td>Security Manager</td>
<td>20+ Years</td>
<td>Risk &amp; IOL</td>
</tr>
<tr>
<td>P8_Mng_Risk</td>
<td>Information Technology and Services</td>
<td>Security Manager</td>
<td>15+ Years</td>
<td>Risk &amp; IOL</td>
</tr>
<tr>
<td>P9_Mng_Risk</td>
<td>Financial (Banking)</td>
<td>Security Manager</td>
<td>12+ Years</td>
<td>Risk &amp; IOL</td>
</tr>
<tr>
<td>P10_Mng_Risk</td>
<td>Consultancy</td>
<td>Security Manager</td>
<td>10+ Years</td>
<td>Risk &amp; IOL</td>
</tr>
<tr>
<td>P11_Cons_Risk</td>
<td>Consultancy</td>
<td>Security Consultant</td>
<td>5+ Years</td>
<td>Risk &amp; IOL</td>
</tr>
<tr>
<td>P12_Cons_Risk</td>
<td>Financial (Banking)</td>
<td>Security Consultant</td>
<td>5+ Years</td>
<td>Risk</td>
</tr>
<tr>
<td>P13_Mng_ISTA</td>
<td>Government agency</td>
<td>Security Manager</td>
<td>15+ Years</td>
<td>ISTA &amp; IOL</td>
</tr>
<tr>
<td>P14_Mng_ISTA</td>
<td>IT Services</td>
<td>Security Manager</td>
<td>5+ Years</td>
<td>ISTA &amp; IOL</td>
</tr>
<tr>
<td>P15_Mng_ISTA</td>
<td>Insurance</td>
<td>Security Manager</td>
<td>20+ Years</td>
<td>ISTA &amp; IOL</td>
</tr>
<tr>
<td>P16_Mng_ISTA</td>
<td>Automotive</td>
<td>Chief Information Security Officer</td>
<td>10+ Years</td>
<td>ISTA &amp; IOL</td>
</tr>
<tr>
<td>P17_Mng_ISTA</td>
<td>Banking</td>
<td>Security Awareness Manager</td>
<td>10+ Years</td>
<td>ISTA &amp; IOL</td>
</tr>
<tr>
<td>P18_Mng_ISTA</td>
<td>Banking</td>
<td>Security Awareness Manager</td>
<td>9+ Years</td>
<td>ISTA &amp; IOL</td>
</tr>
<tr>
<td>P19_Mng_IR</td>
<td>Financial</td>
<td>Insider Threat Detection Leader</td>
<td>15+ Years</td>
<td>IR &amp; IOL</td>
</tr>
<tr>
<td>P20_Cons_IR</td>
<td>Information Technology and Services</td>
<td>Security Consultant</td>
<td>10+ Years</td>
<td>IR &amp; IOL</td>
</tr>
<tr>
<td>P21_Cons_IR</td>
<td>Transport</td>
<td>Security Consultant</td>
<td>10+ Years</td>
<td>IR &amp; IOL</td>
</tr>
<tr>
<td>P22_Mng_IR</td>
<td>Consultancy</td>
<td>Information Security Analyst</td>
<td>15+ Years</td>
<td>IR &amp; IOL</td>
</tr>
<tr>
<td>P23_Mng_IR</td>
<td>Environmental and Civil Infrastructure Services</td>
<td>IT Risk &amp; Assurance Manager</td>
<td>15+ Years</td>
<td>IR &amp; IOL</td>
</tr>
<tr>
<td>P24_Mng_IOL</td>
<td>IT Services</td>
<td>Security Manager</td>
<td>5+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P25_Mng_IOL</td>
<td>Financial Services</td>
<td>Senior security Architect</td>
<td>9+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P26_Mng_IOL</td>
<td>Information Technology and Services</td>
<td>Security Architect</td>
<td>10+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P27_Cons_IOL</td>
<td>Consultancy</td>
<td>Security Consultant</td>
<td>7+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P28_Mng_IOL</td>
<td>Telecommunication</td>
<td>Security Manager</td>
<td>10+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P29_Mng_IOL</td>
<td>Consultancy -Information Technology</td>
<td>Security Manager</td>
<td>15+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P30_Mng</td>
<td>Banking</td>
<td>Chief Security Officer</td>
<td>20+ Years</td>
<td>ISM</td>
</tr>
<tr>
<td>P31_Cons</td>
<td>Consultancy – information security</td>
<td>Principle consultant</td>
<td>10+ Years</td>
<td>ISM standards</td>
</tr>
<tr>
<td>P32_Mng</td>
<td>Telecommunication</td>
<td>Chief Security Officer</td>
<td>15+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P33_Mng_IOL</td>
<td>Telecommunication</td>
<td>Security Risk Consultant</td>
<td>10+ Years</td>
<td>ISM &amp; IOL</td>
</tr>
<tr>
<td>P34_Cons_IOL</td>
<td>cyber security consultancy</td>
<td>Security Consultant</td>
<td>10+ Years</td>
<td>IOL, ISTA and risk.</td>
</tr>
</tbody>
</table>
Most of the interviews were audio recorded. However, in occasional cases the participant did not consent to the interview being recorded to protect the privacy of their current and/or previous clients as well as their own organisation as he/she was signatory to a non-disclosure agreement. In this case, the researcher took notes during the interviews and then the notes were provided to the participants to take their approval to use the information in the research.

3.5.2 Final validation (Follow up interviews)
In the final validation, the refined framework of each area was sent again to the experts who were interviewed in the first data collection stage. The experts of each area were asked to review and provide comments on the practices and activities of each area. An email containing the area framework, followed by several questions on the framework were sent to the participants. Further, an intra-organisational liaison framework which was developed based on the interviewees answers on communication with internal stakeholders was also sent to all participants with several related questions. The participants’ comments and feedback were analysed and used to validate the framework of ISMP areas.

3.6 Data analysis
The interviews were transcribed, and detailed analysis was undertaken to gain an understanding of the managerial activities the participants undertake as part of their job. This resulted in approximately 250 pages of transcribed text. The analysis was conducted based on the theoretical themes that were identified in the conceptual framework. Then, the written text was exported to NVivo (version 11) to help in further coding and categorising. NVivo allows for the development of a very advanced matrix. It provides many quotations in each theme for each interview and by clicking the cell it shows the quotations. The advantage of NVivo matrices is the flexibility and ease of changing the rows and columns, adding new interviews, adding and altering themes. At the first-level coding, the interviews were coded into general ISMPs themes undertaken within each area of ISM. Then the analysis was undertaken one level down to explore the activities within each practice.

Further details of the analysis process and the findings that related to each ISMP area will be presented in the analysis and finding sections in the corresponding chapter of the area (chapter 5 to 8).
3.7 Summary
This chapter presented and explained the research methods and design for this research project. This research project is exploratory and theory building, and develops a framework to guide organisations in implementing comprehensive and effective ISMPs. An interpretive qualitative research approach is adopted in this research project. In order to answer the research question, the research consists of three phases: a contextual study, a conceptual study, and an empirical study. In the contextual study, undertaken in Chapter 2, the research problem, aims and research question were defined. The conceptual study involves conducting a comprehensive review of the literature. The analysis of the literature in this phase resulted in the development of a preliminary framework of ISMPs. In the third and final phase of this research, the preliminary framework of ISMPs is validated and refined by conducting semi-structured interviews with thirty-four Melbourne-based information security management experts. The following chapter discusses the conceptual phase of the study. It presents the overall development process of the proposed ISMP framework.
Chapter 4 FRAMEWORK DEVELOPMENT

4.1 Introduction
The previous chapter provided an overview of the research design adopted in this research project. This chapter introduces the overall information security management practices (ISMPs) framework that was developed based on an extensive review and synthesis of knowledge of the information security management (ISM) literature. The chapter provides information on how the systems theory approach was used in developing a holistic understanding of the ISM. Further, it explains the results of the analysis of the literature. This includes the identification of ISM areas and practices within each area.

4.2 Systems theory approach to information security management in organisations: preliminary conceptual framework of ISM
A system consists of three parts: input variables, processes and output (IOP). Input variables are transformed to outputs through processes. Actions are considered processes, and inputs are factors affecting actions. The IPO model has been adopted in many studies (e.g., Hackman & Morris, 1974; Ilgen, Hollenbeck, Johnson, & Jundt, 2005; Marks, Mathieu, & Zaccaro, 2001).

As discussed Section 3.2.3.1, the use of the systems theory has assisted the researcher to view information security management in a holistic manner. This has enabled the researcher to draw the boundaries between the ISM process itself, and the inputs and outputs of the ISM process. The general review of the ISM literature which was conducted as part of the conceptual phase of this research (see Section 3.4) has resulted in identifying factors that influence the ISM process and elements of ISM process. As depicted in Figure 4-1, the preliminary conceptual framework of the ISM process is based on systems theory and consists of four key components:
Factors influence ISMP
Principles that influence ISMPs may include:
- Information security strategy
- Information security governance
- Compliance and regulatory Requirements

Figure 4-1 Preliminary conceptual framework of ISM process in organisations

- Input

The input component of the IPO model includes information security strategy, information security governance, and compliance and regulatory considerations. These are higher level decision making that inform and influence how organisations practice their information security management. They will not be the focus on this research project.

- Information security strategy

Information security strategy is the first factor that influences the information security management process which was identified from the comprehensive review of the literature. Sangseo and Ruighaver (2008) define information security strategy as the “art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defense organisation’s information infrastructure(s) against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while to be effective” (p.27). Implementing an information security strategy includes the establishment of a comprehensive framework to enable the development, institutionalization, assessment, and improvement of an information security program (Ahmad, Maynard, & Park, 2012; Baskerville, Dhillon, Straub, & Goodman, 2008). The organisation’s information security strategy must support the overall organisation’s
strategic plans with its content clearly traceable to these higher-level sources (Bowen, Hash, & Wilson, 2006; Ezingeard & Bowen-Schrire, 2007; Onibere, Ahmad, & Maynard, 2017).

There are several security strategies that organisations can adopt to address security risk and protect their information resources such as: detection, deterrence, and deception (Ahmad, Maynard, et al., 2012; Ahmad, Ruighaver, & Teo, 2005; Straub & Welke, 1998). The type of information security strategy that an organisation implement has a significant influence on the process of managing information security in the organisations (Ahmad, Tscherning, Bosua, & Scheepers, 2015; Baskerville et al., 2008; Seeholzer, 2012). This is because information security strategy advises organisations to select appropriate measures to best utilize in a most effective and to coordinate each security measure in align with the business goals and objectives (Sangseo, Ahmad, & Ruighaver, 2010). For example, prevention is a security strategy which aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure. Prevention is considered to be the main strategy that is implemented by organisations through using a range of technical and non-technical controls (Ahmad, Maynard, et al., 2012).

- **Information security Governance**

The second factor that influences how organisations manage their information security program is information security governance (Whitman & Mattord, 2014; Yaokumah, 2014). Information security governance is a subset of the overall all cooperate governance that include the adoption of a comprehensive approach to organise effort and integrate various information security practices (Williams, 2001). This aims to provide strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security program (Whitman & Mattord, 2014).

The implementation of an information security governance framework ensures that information security issues are addressed and supported from the highest organisational level (ISACA, 2013). Senior management and the board of directors are accountable for information security governance and must provide the necessary leadership, organisational structures and processes to ensure that information security governance is an integral and transparent part of enterprise governance (Hodgkinson et al., 2010; Trim, 2014). An information security governance framework serves as methodology to implement the organisation’s information security strategies (A. M. Ahmad, 2010).
One of the main elements of the information security governance is to establish an organisational structure for information security (Whitman & Mattord, 2014). This includes defining roles and responsibilities for information security (Chief information officer and chief information security officer) and determining the location of the security function inside the organisations (Dhillon et al., 2007). Another element is establishing steering committees, allocating resources and developing performance measures for the effectiveness of the information security program in organisations (von Solms & von Solms, 2006). All these elements of information security governance have a significant effect on the management process of information security in organisations. Therefore, information security governance is regarded to be an input to the process in the IPO model.

- **Compliance and regulatory requirements**

Another factor that is considered as an input to the ISM process is the compliance and regulatory requirements (Tan, Ruighaver, & Ahmad, 2010). There are many information security laws, regulation and guidelines that organisations either opt to or require complying with (Al-Ahmad & Mohammad, 2013; Susanto, Almunawar, & Tuan, 2011). These security laws, regulation and guidelines can be broadly applicable (i.e., Payment Card Industry Data Security Standard (PCI DSS)), industry-specific guidelines and requirements (i.e., Health Insurance Portability and Accountability Act (HIPAA)) and country specific or international laws (i.e., European Union Data Protection Directive; Safe Harbor Act) (Wüpper & Windhorst, 2012).

Complying with law, regulations, and guidelines involves identifying their requirements and incorporate those requirement into the information security program in organisations (Palmer, Robinson, Patilla, & Moser, 2001). For instance, to comply with ISO/IED 27001, the organisation has to develop information security policies and establish information security training and awareness program (Al-Ahmad & Mohammad, 2013). Internal and external audits are periodically (i.e., every six months or annually) conducted to ensure that the organisation is fulfilling compliance and regulatory requirements (Susanto et al., 2011). The audit process is a systematic assessment of the information security program in an organisation through interviewing staff, reviewing documents and controls (Ahmad & Ruighaver, 2002). Therefore, compliance and regulatory requirements has a great influence on how the organisation manage their information security program (Siponen & Willison, 2009).

- **Process**
Several researchers have argued that information security is a process (Purser, 2004a; Qingxiong et al., 2008). ISM is the overall process of providing protection to organisational information assets. It aims to achieve and maintain an adequate level of, integrity, confidentiality and availability of information and systems (Soomro et al., 2016). Caelli, Longley, and Shain (1991) asserted that ISM is the process of planning, organising and commanding, coordinating, and controlling to establish an adequate level of security. (Savola et al., 2006) also stated that ISM is a process that consists of related activities and information flows between these activities. The process component includes key ISM process identified in the literature. The process part of the model is the main focus of this research project.

- **Output**

The final component, the output of the processes, is the desirable outcome of the overall process of ISM. Each area of ISMP has its specific outcome. For example, the output of policy management is clear management direction to employees in information security related issues, while the outcome of the security education, training, and awareness management is to raise the employees’ awareness about risk and provide them with adequate knowledge and skills to perform their job securely.

- **Feedback loop**

It is important to note that the implementation of ISMPs is iterative. Constant review and assessment are needed to ensure improved implementation of ISMPs. Therefore, the model includes feedback loops. Feedback is essential to ensure that the goals and objectives of each area of ISMP is achieved and ultimately the overall protection of the organisational information resources.

As discussed in the scope of the research (see section 1.6), this research project focuses on managerial practices and activities implemented by organisations to manage their information security. These managerial practices fall under the process component of the ISMP model (see Figure 4-1). Therefore, this research project will focus on the process component while the input and output components of the ISMP model are out of the defined scope of this research.

### 4.3 Review and analysis of the ISMPs in the literature

As described in Section 3.4, two rounds of comprehensive literature review were conducted in this research project. The first round was a general search in ISM literature to identify ISMPs.
The analysis of the related articles led to the identification of four areas of information security management. The second review focused on the literature of the specific areas of ISM. The next two sections describe the analysis and results of the two rounds of the literature review.

4.3.1 The first round of the literature review process: General review of ISM literature

A comprehensive and rigorous review of the information security literature was conducted focusing on two sources: 1) papers published in both the academic and professional literatures, and 2) textbooks (both title and content area) on the topic of information security management. For both academic and professional literature, this research used the following keywords to search SpringerLink, IEEE Xplore, ScienceDirect, the ACM digital library, ProQuest and Google Scholar: ‘information security’, ‘information systems security’, information technology security’, ‘information security management’, ‘cyber security’, ‘information assurance’, ‘information security practices’, ‘information security management practices’, and ‘security practices’. The preliminary results consisted of 496 scholarly articles, industry standards, and technical reports. A review of abstracts resulted in the elimination of 212 papers that were not related to ISMPs, leaving 284 ISMP-related papers.


Content analysis was used to decide which articles contribute significantly to the field of ISM. An open coding process was followed to categorise the contents thematically. During the analysis of the papers, any management-level activity that organisations could implement to achieve information security objectives was determined to be potentially an ISMP. This produced a large number of ISMPs. As the analysis continued, the ISMPs were grouped with guidance from the textbooks for categorisation purposes. This resulted in an imbalance of ISMP within each category – with a high number in categories in which there is much research (e.g., policy and risk management) and fewer in categories where there is less research (e.g. inter-organisational liaison). This reinforces the view of Lim et al (2012) and Choobineh et al. (2007)
who state that the focus of papers tends to be on individual ISMPs rather than on the provision of a rigorous collection of practices.

Regarding the problem of categorising the areas of practice, the research synthesised the various perspectives of the textbooks to help in the analysis process which lead to four key categories: security policy, information security risk management, security incident response, and security education, and training and awareness. Table 4-1 summarises the ISMP areas. These areas are discussed in the following sub-section.

Table 4-1 Summary of Literature Review of ISMPs

<table>
<thead>
<tr>
<th>ISMPs Areas</th>
<th>Representative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security risk management</td>
<td>Finne (2000); Gerber &amp; von Solms (2005); Shedden et al. 2010; Stoneburner et al. 2002; Tsoumas &amp; Tryfonas (2004); Wright (1999); Zafar et al. (2014)</td>
</tr>
<tr>
<td>Information security policy management</td>
<td>Doherty &amp; Fulford (2006); Gaunt (1998); Karyda et al. (2005); Knapp et al. (2009); Ølnes (1994); Rees et al. (2003); Whitman (2008); Whitman &amp; Mattord (2010, 2011a, 2011b)</td>
</tr>
<tr>
<td>Information security training and awareness management</td>
<td>Tsohou et al. (2008); Tsohou et al. (2010b); Waly et al. (2012); Whitman (2008); Whitman &amp; Mattord (2010, 2011a, 2011b); Wilson &amp; Hash (2003)</td>
</tr>
<tr>
<td>Security incident response management</td>
<td>Grance et al. (2004); ISO/IEC18044 (2006); Northcutt (2003); Shedden et al. (2011); Tan et al. (2003)</td>
</tr>
</tbody>
</table>

4.3.1.1 Information security management practice areas

This section presents the ISMP areas as identified in the first round of the comprehensive literature review process. A brief description of ISMP areas is provided in this section and further discussion and literature about the ISMP areas and practices within each area will be provided in subsequent chapters (Chapter 5-8).

1) Information security risk management

ISO/IEC27005 (2012) defines risk management as “coordinated activities to direct and control an organisation with regard to risk” (p. 8) and describes the risk management process as “a continuous process for systematically identifying, analysing, treating, and monitoring risk throughout the life cycle of a product or service” (p. 8). Risk management consists of four main processes: risk assessment, risk treatment, risk acceptance and risk communication (Stoneburner et al. 2002). Each of these risk management processes has a set of practices that should be performed to ensure the protection of organisations (Finne 2000; Gerber et al. 2005; Shedden et al. 2010). For example, conducting a risk assessment includes identifying threats and vulnerabilities in organisational information systems, determining the risk to organisational
assets, and analysing risk. Information security managers have the key responsibility of managing information security risk in an organisation by undertaken risk management practices (Stoneburner et al. 2002; Whitman & Mattord 2010).

2) **Information security policy management**

The ISM and information security literature in general discuss information security policy (ISP) and the importance of providing organisations with management guidelines and directions for information security (Knapp et al. 2009; Ruighaver et al. 2010). ISP is an essential element of an effective ISM program (Doherty et al. 2006; Rees et al. 2003). Rees et al. (2003) proposed a framework of ISP that includes administering an ISP during the development, implementation and evaluation processes. Each of these ISP management processes includes a number of practices undertaken by an organisation’s security managers. Examples of these practices include forming an ISP development team, assessing the current ISPs and identifying the organisation’s security requirements to establish an ISP (Ølnes 1994; Rees et al. 2003; Whitman 2008; Whitman & Mattord 2010).

3) **Information security training and awareness management**

Information security training and awareness (ISTA) programs have a significant role in protecting the organisation’s assets (Nosworthy 2000; Tsohou et al. 2008). ISTA enables employees to comply with information security policy and procedures (Puhakainen et al. 2010; Wilson & Hash 2003). A significant proportion of security incidents are caused by employees’ lack of awareness, which leads to the misuse or misinterpretation of technology or procedures. Thus, ISTA management is a crucial part of ISMPs (Tsohou et al. 2010b). ISTA management includes practices such as managing the design and implementation of these programs and assessing their outcome (Wilson & Hash 2003). Whitman (2003) suggests that one of the practices “that should be developed early is the design and implementation of an employee security education, training, and awareness program” (p95). The ISTA programs should be effectively designed and conducted to positively influence employee’s behaviour towards information security. People are an important element in protecting an organisation’s security; therefore, they should be appropriately trained and educated about information security issues. ISTA management involves the active promotion of ISTA programs as a part of ISM systems (Spurling 1995).
4) Information security incident response management

Regardless of the information security controls that organisations implement, the elimination of security incidents cannot be guaranteed. Recent security reports have shown an increase in the number of security incidents, both internal and external (Baker et al. 2013; Richardson 2010). Therefore, incident response management is critical to ISM (Grance et al. 2004; ISO/IEC18044 2006). It aims to effectively manage the response to security incidents to minimise their impact and protect organisations. Ahmad et al. (2012a) state that the response process consists of five main practices, namely “preparation for, identification, containment, eradication and recovery from incidents” (p.643). Appropriate and effective incident management is important to reduce the impact of threats and maintain business continuity. Security managers should lead and manage the incident response process and have adequate skills and knowledge to manage incident response teams (Werlinger et al. 2010).

4.3.2 The second round of the literature review process: Focused on ISMP areas

The aim of the second round of the search is to thoroughly and comprehensively review the literature for each area of ISMP. The analysis and coding process of the related literature within each area resulted in the development of the preliminarily ISMP framework on each specific ISMP area. The overall understanding that emerged from the systematic review and coding process of all ISMP areas resulted in the development of the ISMP framework. Following is a general description the analysis and review process of the literature of each ISMP area of and specific details related to each ISMP area will be provided in its corresponding chapter.

A comprehensive and rigorous review of each ISMP area was conducted. The review process was guided by the definition of the ISM area. The preliminary results consisted of scholarly articles, industry standards, and technical reports. A review of abstracts resulted in the elimination of papers that were not related to the ISMP area. Related papers were reviewed and then divided into two main categories:

- The first category consists of publications that present lifecycles, guidelines and standards in which several activities were provided to guide organisations on this specific ISMP area. For example, the search in the ISP management area has identified twenty publications related to the development process of ISP; fourteen articles (journal and book sections) propose security policy lifecycles.
• The second category consists of publications that discuss specific aspects of the ISMP areas. In the ISP management area, the second category includes publications that discuss specific aspects of ISP such as policy quality, compliance and employees’ attitude towards security policy.

The guidelines proposed by Okoli and Schabram (2010) were followed to review and analyse the literature. The review process focused on the publications of the first category. Each article was reviewed, paragraphs were reduced into themes, and sentences that related to ISMPs were underlined. Then, ideas and concepts were recorded in the margins. Once the entire paper was reviewed, the important concepts were summarised on the last page. The summaries enabled the researcher by the end of the overall review to remember the important themes discussed throughout the paper. After all publications in the first category were reviewed, the coding process was used to synthesise the articles. The coding process included open, axial, and selective coding, as described in Neuman (2006).

The second review started with more focus on the underlined excerpts, and summaries resulting from the first review. Themes related to the specific ISMP area (i.e., policy management) began to emerge. The researcher reviewed the identified themes, giving more attention to themes that are frequently discussed throughout the articles. Themes were divided into subthemes, and several related concepts were combined into more general concepts. A comparison was made between the themes that reappear in different places.

A similar process was applied to review publications within the second category that do not directly address the development process ISMP area. However, the review process was informed by the result of the review of the first category. Although, no new themes were identified, the review provided more details about the identified themes from publications within the first category, and located evidence to support the identified themes. For example, some ISP lifecycles mention the importance of involving stakeholders in the development process of an ISP. However, they did not identify who the stakeholders were, nor did they discuss their roles and responsibilities in the ISP development process. These details were identified in the second category publications.

As mentioned earlier, the review process was guided by the definition of ISMPs within each area. ISMPs are defined as the strategic-level activities undertaken to manage the ISMP areas (policy, risk, ISTA, incident response) in organisations. Managing security ISM areas involves the development, implementation, and evaluation of the areas.
Identifying related publications in policy management (124 publications), risk management (109 publications), incident management (76 publications) and ISTA management (121 publications) was a relatively easy task as considerable research has been devoted to each individual area. The challenge, however, was to analyse and synthesize knowledge related to ISMPs to develop a more comprehensive and robust understanding of the phenomenon.

4.3.3 Institutionalisation stages of the ISMP framework

This section provides justification for the decision to categorise ISMPs within each area of ISM into three institutionalisation stages: 1) the Development stage, 2) the Implementation and Maintenance stage, and 3) the Evaluation stage.

The management textbooks provided two distinct contributions that allowed us to categorise the ISMPs. From Whitman and Mattord (2010) it was learnt that since information security is implemented through a process of institutionalisation, ISMPs can be categorised in terms of the particular phase in the process lifecycle (e.g. develop, implement & maintain, evaluate). The second contribution was a useful categorisation of the topic areas in ISM that align with the definition of management practices (examples include information security risk management, information security policy, and incident response).

Whitman and Mattord (2010) point out that information security in general can only be implemented through a process of institutionalisation. They propose a security system development lifecycle (SecSDLC) consisting of six phases (investigation, analysis, logical design, physical design, implementation, and maintenance and change) designed to implement an information security project in an organisation. The SecSDLC lifecycle engages in an analysis of the full-spectrum of controls (managerial and technical) already in place in an organisation before engaging in the design of a new blueprint that is ultimately implemented to achieve new security objectives.

Unlike the SecSDLC lifecycle, which adopts a project-oriented view of the full spectrum of security controls, this project takes a process-oriented view within the narrow scope of ISM, with the aim of developing a framework of practices (rather than a method for implementation). However, the concept of institutionalisation applies to implementation of managerial practices as much as it does to security systems. Since the process-oriented view does not consider project implementation, the research proposes the project-specific stages of investigation, analysis, logical design, and physical design be replaced with the proposition that management functions
in general undergo ‘development’. Since management functions, must be implemented in the organisation, ‘implementation’ and ‘maintenance’ are also relevant to the process-oriented view. Whitman and Mattord (2010) suggest that information security measures must ‘change’ to adapt to the information security environment. From a process point of view this concept has been incorporated in the notion of ‘evaluation’ which focuses on the need for feedback and improvement of management functions. There is support for this kind of categorisation in academic literature. Some academic papers (e.g. Rees et al. 2003) discuss practices related to the development of security policy whereas others (e.g. Gaunt 1998) have focused on the practices related to implementation of security policy. Still others (e.g. Whitman 2008) discuss the importance of evaluating security policy to ensure its effectiveness.

The use of the lifecycle approach in the ISM literature is very common. It is very beneficial as it allows good management of the process of (e.g., ISP development and ISTA management) and assures managers that all important activities for the development process are performed (Maynard and Ruighaver 2007; Patrick 2002). Ølnes (1994) stresses the importance of having a methodological approach in developing, implementing and maintaining ISP. Further, Patrick (2002) argues that the use of an ISP lifecycle approach will ensure a comprehensive development process that encompasses all required activities to develop an effective security policy. Chen, Sharman, Raghav Rao, and Upadhyaya (2008) also stated that “A lifecycle approach provides a broad and systematic view of the activities relating to emergency response management” (p.68).

Therefore, the research proposes that institutionalisation of information security management takes place in distinct stages. The process must be: 1) developed, 2) implemented and maintained in the organisation. Further, the process must undergo 3) evaluation for the purpose of feedback and improvement. These three institutionalisation stages provide structure for the framework. As per the previous example, the academic literature related to specific ISMP areas tends to also make these distinctions. These three institutionalisation stages will be used across all ISMP areas.

### 4.4 Proposed information security management practices framework

As a result of the analysis process of the academic and professional literatures, along with the use of textbooks to guide the analysis, a preliminary ISMP framework was developed. The framework identifies four areas of management practice. Within each area, the stages of
institutionalisation are listed, and a representative management practice is shown for illustrative purposes. The next four chapters will introduce the result of the literature analysis and present the preliminary ISMP framework for each ISMP area (chapters 5 to 8).

Table 4-2 The top-level of the preliminary framework of Information Security Management Practices

<table>
<thead>
<tr>
<th>Practice Area</th>
<th>Institutionalisation Stage</th>
<th>Representative examples of practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policy</td>
<td>Develop</td>
<td>Assess existing organisational policies (Rees et al. 2003)</td>
</tr>
<tr>
<td></td>
<td>Implement &amp; Maintain</td>
<td>Distribute policy (Whitman &amp; Mattord 2010)</td>
</tr>
<tr>
<td></td>
<td>Evaluate</td>
<td>Review policy periodically (Knapp et al. 2009).</td>
</tr>
<tr>
<td>Information security</td>
<td>Develop</td>
<td>Develop risk management plan (NIST 2011)</td>
</tr>
<tr>
<td>risk management</td>
<td>Implement &amp; Maintain</td>
<td>Conduct risk assessment (Humphreys 2008)</td>
</tr>
<tr>
<td></td>
<td>Evaluate</td>
<td>Review risk management plan (Stoneburner et al. 2002)</td>
</tr>
<tr>
<td>Security incident response</td>
<td>Develop</td>
<td>Form incident response team (Ahmad et al. 2012a)</td>
</tr>
<tr>
<td></td>
<td>Implement &amp; Maintain</td>
<td>Deploy the incident response team (Mitropoulos et al. 2006)</td>
</tr>
<tr>
<td></td>
<td>Evaluate</td>
<td>Review security incident response plan (Grance et al. 2004)</td>
</tr>
<tr>
<td>Security training and</td>
<td>Develop</td>
<td>Conduct a ISTA needs Assessment (Wilson &amp; Hash 2003)</td>
</tr>
<tr>
<td>awareness</td>
<td>Implement &amp; Maintain</td>
<td>Conduct ISTA program using available delivery techniques (Whitman &amp; Mattord 2010)</td>
</tr>
<tr>
<td></td>
<td>Evaluate</td>
<td>Review ISTA programs periodically (Wilson &amp; Hash 2003)</td>
</tr>
</tbody>
</table>

This research project focuses on ISMPs. The ISMP framework is an important step in the maturity of ISMPs in organisations. It will allow organisations to implement a program of information security management with sufficient guidance in order to meet their security objectives. Organisations will be able to use the framework as a guide to the practices that are required within each ISMP area, and will be able to self-select practices to be followed depending on the organisation’s information security requirements. They may also determine whether some of these ISMPs could be outsourced, depending on a variety of factors, including organisation size, the organisations risk propensity and their in-house expertise. The ISMP framework will be able to be further used by organisations as a benchmarking tool against which improvement in existing ISMPs can be assessed.

The proposed framework will also allow organisations to implement ISMPs in a more coherent and consistent approach by identifying relationships between practices and provide guidance to organisations on how to implement ISMP in a comprehensive and collective manner.
4.5 Summary
This chapter presented the conceptual analysis and explained the process of analysing and synthesising the literature to develop an ISMP framework. It consisted of two main parts. The first part discussed how the systems theory approach assisted the researcher to establish an overall understanding of the ISM area, while the second part provided a detailed explanation of the analysis of the literature which led to identifying areas of ISMP and practices of each area. In addition, the chapter provided justification of the decision to use three institutionalisation stages, the development stage, the implementation and maintenance stage and the evaluation stage across all areas of ISMP.

The next four chapters will discuss ISMP areas. Each chapter will consist of six parts:

i. Introduction of the ISMP area:
This part includes the research question and the overall structure of the chapter.

ii. Literature review
The literature review section of each chapter provides a background of the ISMP area and related work on existing frameworks and development lifecycles in the literature of each area.

iii. Framework development,
The framework development section of each chapter (5-8) presents the result of the conceptual study phase 2a which is the comprehensive review and syntheses each ISMP area (See Section 4.3.2). In each chapter, the section presents practices and key activities of the ISMP area.

iv. Data analysis and Findings
This part presents the analysis of empirical data collected to validate the framework of each ISMP area.

v. Final validation
This section provides analysis and findings from the follow up interviews with the participants of each area.

vi. Brief discussion to issues related the area.
This section discusses the main findings of the area and relate them to the existing literature.
Chapter 5 INFORMATION SECURITY RISK MANAGEMENT PRACTICES

5.1 Introduction
The previous chapter focused on the comprehensive review of the information security management (ISM) literature and the development of the research framework using the systems theory. The review resulted in the identification of information security management practices (ISMPs) areas and the development of the preliminary ISMP framework. The aim of this chapter is to identify managerial practices of ISRM and develop a comprehensive framework based on the literature. This is done by: (1) comprehensively reviewing and analysing the information security risk management (ISRM) literature to identify managerial practices in ISRM, and (2) refining the aforementioned framework using the findings from the empirical study.

This chapter is organised as follows. Section 5.2 provides an overview of the existing literature of ISRM, highlighting related topics and issues. Section 5.3 presents the proposed framework for ISRM practices. Section 5.4 presents empirical data from expert interviews that were conducted to refine the proposed framework. Section 5.5 presents the analysis and findings from the follow up interviews which were conducted for final validation of the framework. Section 5.6 discusses the contribution and implications of the proposed framework of ISRM practices. Section 5.7 provides a summary of the chapter.

5.2 Literature review
The increased reliance on information systems has increased the exposure to risks. ISRM is defined as a “process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organisations’ missions.” (NIST, 2006, p.84). This definition represents
a strategic view of the risk management process. It encompasses balancing the operational and economic costs of the recommended controls to achieve the organisation’s mission.

ISRM is an iterative process (Fenz & Ekelhart, 2011; Zafar et al., 2014). It aims to assist organisations to identify major risks and implement appropriate security controls (technological and managerial) to protect their systems (Lalonde & Boiral, 2012; Raz & Hillson, 2005). In addition ISRM increases the organisation awareness of risks (Sahlin-Andersson, Scheytt, Soin, & Power, 2006).

ISRM is an important part of the information security framework (Dhillon, 2007b; Whitman & Mattord, 2008). It should be integrated with other ISMP areas: ISP, ISTA, and incident response (Dhillon, 2007b; Zafar et al., 2014). In fact, all these security areas depend on the results of ISRM. For example, in order to develop an ISP, organisations need to have a recent security assessment as an input to the development process (Wiant, 2005)(See Chapter 6 on information security policy management). ISO 31000 stated that risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient (AS/NZS ISO 31000:2009). The risk management process should become part of, and not separate from, those organisational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

The importance of the ISRM area has prompted academics and professionals to dedicate considerable effort to improving the organisations’ ISRM process. Several standards and guidelines (e.g. ISO 27005, NIST 800-59, OCTAVE and ENISA) have been developed to assist organisations to manage their information security risks effectively.

Subsequent research has been conducted to explain and analyse existing ISRM standards, and how these standards and guidelines can be implemented in organisations. A number of studies (e.g., Eloff, Labuschagne, & Badenhorst, 1993; Raz & Hillson, 2005) have focused on comparing and analysing phases and activities of current ISRM approaches.

Several studies (e.g., Baskerville, 1991; Pan & Tomlinson, 2016; Webb et al., 2014, 2016) have focused on the risk assessment process which is considered to be the core of the organisation’s ISRM process. These studies investigated how organisations conduct risk assessment and the quality of the risk assessment practice in organisations.
Compared to research on the development of the ISRM approaches and methodologies and for risk assessment, the planning (context establishment) phase and the evaluation of the process has received little attention. While a few studies have discussed the importance of evaluating the ISRM process, the review did not identify any studies that primarily focused on planning and preparation activities as part of the ISRM process.

5.2.1 Overview of existing ISRM standards

Several researchers recommend organisations adopt an ISRM approach that enables them to manage their risks effectively (Fenz, Heurix, Neubauer, & Pechstein, 2014; Lalonde & Boiral, 2012; Raz & Hillson, 2005; Whitman & Mattord, 2008). There are a number of widely accepted standards and guidelines, such as ISO 27005, NIST 800-59, OCTAVE and ENISA. Whilst these standards present different ISRM approaches, processes and methodologies, they all contain the same activities (in varying levels of abstraction), granularity, terminology, and semantics. These common activities can be grouped into several phases: context establishment, risk assessment, and review and monitoring of information security risks and their factors (Al-Ahmad & Mohammad, 2013; Fenz & Ekelhart, 2011; Fenz et al., 2014; Lalonde & Boiral, 2012; Raz & Hillson, 2005). Following is a discussion and description of each of the abovementioned phases:

• The context establishment phase

The context establishment phase in ISO 27005 corresponds to Framing risks in NIST SP 800-39 and the Corporate Risk Management Strategy in ENISA. This phase aims to develop an understanding of the external and internal context for ISRM (Dashti, Giorgini, & Paja, 2017; Fenz et al., 2014). This includes examining the organisation to determine if there are any industry-specific risks as well as any other issues that may impact the ISRM process, or steer it down a particular path. Understanding the context also involves analysing the organisation to ensure that the business environment is known (business type, focus, departments, structure and customers), to align organisational goals with the goals of the information security risk assessment, and to establish what risks may be present in each area of the organisation to better scope and place boundaries on the risk management process to come (Shedden et al., 2006; Shedden, Smith, & Ahmad, 2010). In addition, this phase is very important for integrating the ISRM process with other organisational processes (ENISA, 2012b).

The context establishment phase involves activities such as defining the scope and boundaries for the process and establishing an appropriate organisation for operating the ISRM. Further,
this phase includes developing a risk management strategy that provides guidelines on how the organisation intends to assess risk, respond to risk, and monitor risk. In other words, it involves the development of risk evaluation criteria, impact criteria and risk acceptance criteria (AS/NZS ISO/IEC 27005:2012). In addition, the organisation should ensure the availability of the resources required to conduct the ISRM process (Alcántara & Melgar, 2016).

- The risk assessment phase

Risk assessment is the core of the ISRM process (Baskerville, 1991; Eloff et al., 1993; Shedden, Smith, et al., 2010; Webb et al., 2014). This phase has received considerable attention in the literature compared to other phases. It involves the three main activities of risk identification, risk analysis, and risk evaluation (Caralli, Stevens, Young, & Wilson, 2007; Chen & Wen, 2010; ENISA, 2012b; Ronald S. Ross, 2011). Risk identification aims to identify assets, threats, existing controls, vulnerabilities, and consequences. Risk analysis utilises quantitative and/or qualitative methodology to assign values to the likelihood and consequences of a risk. The risk evaluation step compares risk against risk evaluation criteria and risk acceptance criteria (V. Agrawal, 2017; AS/NZS ISO/IEC 27005:2012).

- The risk treatment phase

In the risk treatment phase, the organisation selects the appropriate action to treat and mitigate risks identified in the assessment phase of the ISRM process (Eloff et al., 1993). It involves developing alternative courses of action to respond to risk, evaluating the alternative courses of action, determining appropriate course of action and implement risk responses (Stoneburner, Goguen, & Feringa, 2002). According to (AS/NZS ISO 31000:2009), there are four treatment options: risk modification, risk retention, risk avoidance, and risk sharing. The output of this step is called the risk treatment plan, which is a list of risks and treatment options. The organisation may decide to accept risk; however, the decision should be made according to acceptance criteria as well as the treatment options (Alberts & Dorofee, 2003; Blakley, McDermott, & Geer, 2001; Finne, 2000).

- The risk monitoring and review phase

The last common phase amongst existing risk management standards is the risk review and monitoring phase (Eloff et al., 1993; Fenz et al., 2014). This phase aims to maintain the effectiveness of the ISRM process by establishing an ongoing monitoring and review process (ENISA, 2012a). The monitoring and review phase involves monitoring identified risks
and the risk environment to detect any changes that may result in a change in the nature of the risk (Ronald S. Ross, 2011). It also involves monitoring the implementation of the risk response plan to determine the effectiveness of risk response measures (Lalonde & Boiral, 2012). It also ensures that the specified management action plans remain relevant and updated (IEC/ISO 31010, 2009).

5.2.2 Issues and challenges in adopting existing ISRM standards

Existing ISRM standards aim to provide a comprehensive approach to managing information security. They play a significant role in improving an organisation’s ISRM practices (Lalonde & Boiral, 2012). However, the fact that there are many risk management standards and guidelines that are available for organisations to adopt has left organisations confused about what to adopt (Al-Ahmad & Mohammad, 2013). The lack of guidance for the process of selecting an ISRM approach/framework has prompted several researchers (Al-Ahmad & Mohammad, 2013; Fenz & Ekelhart, 2011; Fenz et al., 2014; Lalonde & Boiral, 2012; Raz & Hillson, 2005; Shedden et al., 2006) to compare and analyse the existing ISRM approaches. The aim of these studies is to provide guidance to organisations on the selection and implementation of an ISRM approach. For example, Fenz et al. (2014) compared and analysed existing ISRM methodologies. Further, they proposed a generic information security risk methodology based on existing approaches. Similarly, Al-Ahmad and Mohammad (2013) compared some of the existing ISRM according to several criteria: implementation complexity, needed skills, generality, adoption of other organisations, availability of information to guide the implementation, and cost of implementation. Further, the authors proposed a model to aid organisations to select the appropriate ISRM approach.

Although ISRM standards and guidelines have made a significant contribution to improving the ISRM practice in organisations, there are several issues that the organisations are faced with when implementing an ISRM standard (Shedden, Scheepers, Smith, & Ahmad, 2011; Webb et al., 2014). The first issue is that implementation of ISRM standards requires substantial resources and expertise to support the implementation (Shedden, Scheepers, et al., 2011). Therefore, organisations that lack an ISRM system and have constrained resources and expertise find it very challenging to implement the standards in the formal and more complex approach intended by the standards’ designers.

With the aim of understanding how risk assessment is practised in organisations, Shedden, Smith, et al. (2010) conducted three in-depth case studies of organisations claiming to comply
with best-practice information security standards. They found all three organisations had taken an informal and simplistic approach to their implementation of the standard, as opposed to the more complex task of performing a granular assessment in the standard. Shedden et al. (2010) findings support the conclusions of Al-Ahmad and Mohammad (2013), Siponen and Willison (2009) and Tan et al. (2010) who pointed out the problem of motivation to adopt the standards. Siponen (2006) argues that standards compliance only requires that ISRM processes exist; it does not regulate the granularity of the processes themselves. Further, some organisations treat compliance as a goal in itself, rather than as a method for improving their security postures (Acuña, 2017; Matwyshyn, 2009). Tan et al. (2010) argued that it “result in a compliance culture, where those responsible for implementing information security are more interested in complying with organisational standards and policies than improving security itself” (p.55).

Another issue that may hinder the effective implementation of ISRM standards by organisations is the lack of clarity and consistency around terminology and semantics used to describe the ISRM process (Eloff et al., 1993). Professional and academic literature uses different terminologies to refer to the same process. The use of different terminologies to refer to the same activity creates confusion and may affect the implementation. For example, (AS/NZS ISO/IEC 27005:2012) standards refer to risk identification, risk analysis, and risk evaluation as risk assessment. Each of the three activities of risk assessment can be broke down into several tasks. Risk identification, for instance, consists of five tasks: identification of assets, identification of threats, identification of existing controls, identification of vulnerabilities and identification of consequences. However, NIST (Stoneburner et al., 2002) uses risk assessment to describe a methodology that consists of nine steps to identify risk, analyse it and recommend controls, and document the result. Pattinson and Anderson (2006) use ‘risk analysis’ as an overall definition for both analysing and assessing risks.

Further, ranking risks according to their impact and likelihood is referred to in the literature in different terms. Some authors (e.g., Gerber & von Solms, 2005; Ozkan & Karabacak, 2010; Stoneburner et al., 2002) use the term ‘evaluate risk’, while others (HB 167: 2006; IEC/ISO 31010, 2009) use the term ‘analyse risk’. The term ‘assess risk’ is also used to refer to ranking risks. Taking the appropriate action to reduce risks to an acceptable level is also referred to in different terms. Some authors use ‘response’ to risk while others use ‘treat’ risk. The term ‘mitigate’ risk is also used to refer to the same thing. The use of different and conflicting
terminology and semantics in existing ISRM standards and guidelines confuse organisations and may affect the guidance those standards provide.

5.3 Information Security Risk Management Practices framework

As described in Section 4.3.2, to review ISRM literature, a comprehensive search on various databases and search engine was undertaken using terms the following search terms: ‘security risk management’, ‘risk management process’, ‘security risk management methodology’, and ‘risk management practices’. See Section 4.3.2 for more details about the search and analysis process.

The overall understanding that emerged from the comprehensive review and coding process resulted in the development of a model of ISRM management practices. This section discusses the proposed framework. Table 5-1 depicts the framework which consists of three main stages: the Development stage, the Implementation & Maintenance stage, and the Evaluation stage (see Section 4.3.3). Each stage consists of a number practices, each having a number of key activities.

Table 5-1 The preliminary framework of ISTA management practices

<table>
<thead>
<tr>
<th>Stage</th>
<th>Practice</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Establish risk management context</td>
<td>Define goals and objectives of the process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Define scope and boundaries of the process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify required resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify assumptions and constraints</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify relevant stakeholders for security risk management process</td>
</tr>
<tr>
<td></td>
<td>Establish security risk management team</td>
<td>Define roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure the risk management team receives adequate training</td>
</tr>
<tr>
<td></td>
<td>Develop security risk management approach/criteria</td>
<td></td>
</tr>
<tr>
<td>Implement &amp; Maintain</td>
<td>Conduct the risk assessment</td>
<td>Collect risk data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analyse risk data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Take appropriate decision to reduce risk to acceptable level</td>
</tr>
<tr>
<td></td>
<td>Communicate the risk assessment result</td>
<td>Document the results of the analysis and treatment plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Share the result with relevant stakeholders</td>
</tr>
<tr>
<td>Monitor Risk</td>
<td>Review of risk management process</td>
<td>Review risk management approach/criteria</td>
</tr>
<tr>
<td>Evaluate</td>
<td></td>
<td>Measure the effectiveness of risk management practices</td>
</tr>
</tbody>
</table>
5.3.1 The Development Stage

The development stage represents all practices associated with planning and preparing for the ISRM process. The development stage consists of three main practices: (1) establish risk management context, (2) establish information security risk management team, and (3) develop information security risk management approach/criteria.

**ISRM-Practice 1: Establish risk management context**

Establish the ISRM context aims to understand the environment in which the organisation operates (AS/NZS ISO/IEC 27005:2012; Ronald S. Ross, 2011). Understanding the organisation will help to gain knowledge about how internal and external environments affect the organisation exposure to risk, which will allow the organisation to conduct ISRM practices in a manner that appropriate to organisation’s type. According to HB167:206 establishing the context for ISRM provides the scope, parameters, and plan that are required to conduct the risk management process within a specific organisational context. Establishing an ISRM context consists of five key activities: (1) define goals and objectives of the process, (2) define scope and boundaries of the process, (3) identify required resources to conduct the process, (4) identify assumptions and constraints to the process, and (5) identify relevant stakeholders for the ISRM process.

**Practice 1-Activity 1: Define goals and objectives of the process**

To achieve the desired result from an ISRM process in an organisation, the goals and objectives of the process need to be defined clearly (AS/NZS ISO/IEC 27005:2012). This activity includes determining whether the process is an initial or subsequent process (Ronald S. Ross, 2011). The general goal of the ISRM process is to identify major risks and recommend an appropriate action to mitigate these risks. The risk management process should enable better awareness of risks and the importance of managing risks and establishing appropriate security governance to manage such risks (Ronald S. Ross, 2011). The organisation should also set objectives and outcomes from the risk management process (HB 167: 2006).

**Practice 1-Activity 2: Define scope and boundaries of the process**

The scope and boundaries around which the ISRM process will take place need to be defined clearly (Raz & Hillson, 2005; Ronald S. Ross, 2011). The scope and boundaries define the areas of the organisation that will be included in the ISRM process (Microsoft Security Center of Excellence, 2006). The benefit of defining the scope and boundaries of an ISRM process is to
ensure that all relevant assets are taken into consideration in the risk assessment (AS/NZS ISO/IEC 27005:2012). Additionally, defining the boundaries will help to address the risk from these boundaries.

The scope of the ISRM process can involve the entire organisation or one department/operational area in the organisation. It is important that the scope is reasonable: it should not be too broad or too narrow. A too broad scope will make it difficult to manage the information gathering and analysis. A too small scope, on the other hand, will not result in meaningful information (Alberts & Dorofee, 2003). Therefore, the size of the ISRM should be manageable to avoid unnecessary work and improve the quality of the risk assessment process (HB 231: 2004).

Defining the scope and boundaries involves the documentation of all the organisations functions to be included in the ISRM process. The organisation should articulate which part of the organisation will be included in the scope. If it is not possible to include the entire organisation in the scope of the assessment process, it is advisable to start with a well-understood business unit/department which is very beneficial for demonstrating the value of the process and building the momentum (Microsoft Security Center of Excellence, 2006). Once the scope is defined, it should be discussed and thoroughly explained to all relevant stakeholders (Microsoft Security Center of Excellence, 2006).

**Practice 1-Activity 3: Identify required resources to conduct the process**

The literature provides very little information about the resources required for the ISRM process. (AS/NZS ISO/IEC 27005:2012) stated that it is important to identify the required resources to conduct the process. These resources may include technical tools, expertise and budget to conduct the ISRM process (Caralli et al., 2007). The organisation should ensure that the required capability, and resources are available and accessible to support the achievement of the risk management process (HB 167: 2006).

**Practice 1-Activity 4: Identify assumptions and constraints to the process**

Organisations should identify specific assumptions and constrains to the ISRM process within the defined scope (Ronald S. Ross, 2011). This information is essential as it informs and guides the risk assessment process. Assumptions should be made about type of threat sources, threat events, and vulnerabilities that should be considered during process (Stoneburner et al., 2002).
In addition, assumptions should be made about the process for determining likelihood and impacts. Organisations should also determine the level and types of risk that are acceptable.

In terms of constraints, organisations should identify direct and indirect constraints to the process (Ronald S. Ross, 2011). Direct constraints include financial and time limitations, while indirect constraints include legal and cultural limitations. Identifying constraints during the development stage will enable organisations to take into account these constraints during the planning which will result in effective management of information security risks (Stoneburner et al., 2002).

**Practice 1-Activity 5: Identify relevant stakeholders for the ISRM process**

The ISRM process entails ongoing communication and information sharing between the information security team and key organisational stakeholders (HB 327:2010; Stoneburner et al., 2002). Therefore, to manage security risk effectively, stakeholders need to be identified. (AS/NZS ISO/IEC 27005:2012) defines information security risk management stakeholders as “those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk” (p.6). The definition indicates that stakeholders may be internal and/or external to the organisation. Internal stakeholders include all members inside the organisation, such as managers and employees from different departments while external stakeholders include suppliers, customers, business partners, and service providers (Whitman & Mattord, 2008). Table 5-2 provide examples of ISRM stakeholders and their roles in the process.

Ideally, the process of managing risk requires the participation of all members of the organisation. Identifying stakeholders, therefore, will enable the organisation to communicate with those people and encourage them to participate in the ISRM process. In fact, the Microsoft security risk management guide (Microsoft Security Center of Excellence, 2006) considers having a well-defined ISRM stakeholder as one key success factors for the process of managing security risk in the organisation. In the same vein, the findings of Spears and Barki (2010)’s study on user participation in ISRM endorse the importance of involving users in the process of managing security risk. Spears and Barki (2010) argued that the participation of users has a positive effect on ISRM. The involvement of users provides needed knowledge of a business process, which will result in “greater alignment between information security risk management and business environment” (p.503). The alignment will improve the ISRM and, as a result, enable the organisation to implement effective security controls to mitigate risks.
Table 5-2 Example of the ISRM process stakeholders and their roles (Stoneburner et al., 2002).

<table>
<thead>
<tr>
<th>ISRM stakeholders</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Management</td>
<td>Ultimate responsibility for mission accomplishment, must ensure that the necessary resources are available. Assess and incorporate results of the risk assessment activity into the decision-making process.</td>
</tr>
<tr>
<td>Chief Information Officer (CIO)</td>
<td>Responsible for the agency’s IT planning, budgeting, and performance including its information security components.</td>
</tr>
<tr>
<td>System and Information Owners</td>
<td>Responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. The system and information owners must therefore understand their role in the risk management process and fully support this process.</td>
</tr>
<tr>
<td>Business and Functional Managers</td>
<td>The managers responsible for business operations and IT procurement process must take an active role in the risk management process.</td>
</tr>
<tr>
<td>Security managers and computer security officers</td>
<td>Responsible for their organisations’ security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize risks to the IT systems that support their organisations’ missions.</td>
</tr>
<tr>
<td>IT Security Practitioners</td>
<td>Responsible for proper implementation of security requirements in their IT systems.</td>
</tr>
<tr>
<td>Security Awareness Trainers</td>
<td>Develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.</td>
</tr>
</tbody>
</table>

The literature has placed considerable emphasis on the concept of communication and consultation with stakeholders during the process, engaging them, and encouraging them to participate in the process of managing risk and the overall security program. Including stakeholders in the process of managing risk will allow the ISRM team to take into consideration different perspectives, understanding, assumption, and concerns to risk in the organisation (HB 327:2010).

**ISRM-Practice 2: Establish information security risk management team**

The aim of the ISRM team is to facilitate and collaborate with stakeholders in the organisation in planning and implementing risk management activities. Establishing the ISRM team has been overlooked by major standards and guidelines, such as (AS/NZS ISO/IEC 27005:2012) and (Ronald S. Ross, 2011). However, several ISRM approaches such as (Microsoft Security Center of Excellence, 2006) and OCTAVE (Alberts & Dorofee, 2003) consider establishing ISRM team to be an important practice. The team should be an interdisciplinary team that includes both business and information security perspectives (Spears & Barki, 2010). The team should
include people from different groups within the organisation such as business assets owners, users, information security experts, and information technology managers (Spears, 2006).

The ‘Establish information security risk management team’ practice consists of two key activities: (1) Define roles and responsibilities, and (2) Ensure the risk management team receives adequate training.

**Practice 2-Activity 1: Define roles and responsibilities**

Defining the roles and responsibilities of relevant stakeholders is very important. It is a critical success factor for the ISRM process (Prislan, 2014; Ronald S Ross & Johnson, 2010). Clear roles and responsibilities will encourage the participation in the process, prevent conflict that might occur, and hold ISRM team members and key stakeholders accountable if they did not meet their commitments (Microsoft Security Center of Excellence, 2006). Some authors provide some guidance on the roles and responsibilities of key stakeholders including the ISRM team members. For instance, the Microsoft security risk management guide provides a summary of responsibilities in security risk management (See Table 5-3).

**Practice 2-Activity 2: Ensure the risk management team receives adequate training**

The team members should have the knowledge and skills to identify, assess, treat and monitor risks (Alberts & Dorofee, 2003). They should have the ability to include other people from the organisation and external organisations (stakeholders). Team members should have knowledge of the business process and structures of the organisation. They should also have good communication skills to be able to communicate with internal and external stakeholders (Spears & Barki, 2010).

The Microsoft risk management guide discussed the concept of empowerment for the ISRM team. Empowerment requires the allocation of adequate resources and having the authority to take decisions that affect the organisation (Microsoft Security Center of Excellence, 2006). The ISRM team will encounter first-time participants in the risk management process who may not fully understand their roles. Always take the opportunity to provide an overview of the process and its participants. The objective is to build consensus and highlight the fact that every participant has ownership in managing (ISACA, 2013).
<table>
<thead>
<tr>
<th>Title</th>
<th>Primary Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Sponsor</td>
<td>Sponsors all activities associated with managing risk to the business, for example, development, funding, authority, and support for the Security Risk Management Team.</td>
</tr>
<tr>
<td>Business Owner</td>
<td>Is responsible for tangible and intangible assets to the business. Business owners are also accountable for prioritizing business assets and defining levels of impact to assets. Business owners are usually accountable for defining acceptable risk levels; however, the Executive Sponsor owns the final decision incorporating feedback from the Information Security Group.</td>
</tr>
<tr>
<td>Information Security Group</td>
<td>Owns the larger risk management process, including the Assessing Risk and Measuring Program Effectiveness phases. Also defines functional security requirements and measures IT controls and the overall effectiveness of the security risk management program.</td>
</tr>
<tr>
<td>Information Technology Group</td>
<td>Includes IT architecture, engineering, and operations.</td>
</tr>
<tr>
<td>Information security risk management Team</td>
<td>Responsible for driving the overall risk management program. Also responsible for the Assessing Risk phase and prioritizing risks to the business. At a minimum, the team is comprised of a facilitator and note taker.</td>
</tr>
<tr>
<td>Risk Assessment Facilitator</td>
<td>As lead role on the Security Risk Management Team, conducts the data gathering discussions. This role may also lead the entire risk management process.</td>
</tr>
<tr>
<td>Risk Assessment Note Taker</td>
<td>Records detailed risk information during the data gathering discussions.</td>
</tr>
<tr>
<td>Mitigation Owners</td>
<td>Responsible for implementing and sustaining control solutions to manage risk to an acceptable level. Includes the IT Group and, in some cases, Business Owners.</td>
</tr>
<tr>
<td>Security Steering Committee</td>
<td>Comprised of the Security Risk Management Team, representatives from the IT Group, and specific Business Owners. The Executive Sponsor usually chairs this committee. Responsible for selecting mitigation strategies and defining acceptable risk for the business.</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>General term referring to direct and indirect participants in a given process or program; Stakeholders may also include groups outside IT, for example, finance, public relations, and human resources.</td>
</tr>
</tbody>
</table>

**ISRM-Practice 3: Develop security risk management approach/criteria**

The ISRM approach provides overall guidance on various aspects of the ISRM process such as risk assessment, risk treatment, and risk monitoring (Badenhorst & Eloff, 1990; Caralli et al., 2007; HB 231: 2004; Raz & Hillson, 2005). It helps the organisation to have a repeatable process and to build a common perspective or understanding of how risk should be managed (ENISA, 2012b).
In terms of risk assessment, the ISRM approach determines how risk assessment is going to be conducted, what techniques will be used to assess risk, and what data gathering tools are going to be used to collect data about assets, vulnerabilities, and risks (ENISA, 2012b). How the collected data will be analysed and whether the organisation should use quantitative, qualitative or semi-quantitative approach should be also included.

The approach will involve the development of criteria to assist organisations to analyse the identified risks (HB 167: 2006). Criteria will help organisations to make a decision on whether the identified risk is acceptable/tolerated, or it needs to be treated. Having a well develop criteria will help organisations to make transparent, systematic, and repeatable decisions on what risks need to be treated and how to prioritise risks (AS/NZS ISO 31000:2009; Jerman-Blažič, 2008).

ENISA (2012b) stated that the criteria developed to evaluate risk should consider the context of the organisation and the scope of the process and be aligned with the organisation’s policy and support its goals and objectives.

5.3.2 The Implementation and Maintenance Stage

In the implementation and maintenance stage, the risk assessment is conducted and treatment for risks is implemented. The implementation and maintenance stage consists of three key practices: (1) deploy the ISRM team, (2) communicate risk assessment results, and (3) monitor risks.

**ISRM-Practice 4: Conduct the risk assessment**

As explained in Section 5.2.1, the risk assessment phase is the core of the ISRM process. The organisation should provide clear information to the team in regard to scope, relevant stakeholders, and guidelines on how to conduct the ISRM process (AS/NZS ISO/IEC 27005:2012; Baskerville, 1991; ENISA, 2012b; Lange, von Solms, & Gerber, 2016).

The ISRM team should work with stakeholders within the specified scope in the organisation to collect data about assets, vulnerabilities, and threats, and then analyse them. Collaboration with stakeholders is very important for performing these activities in a correct and accurate manner, because stakeholders will have a better understanding of their business unit (critical assets, potential weaknesses, possible scenarios of risk) (Bernard, 2007; Eloff et al., 1993; Spears, 2006; Spears & Barki, 2010).
Organisation deploys the ISRM to start collecting data (assets, vulnerabilities and threats), analyse them, and decide which option should be implemented to reduce the identified risk to acceptable level (Microsoft Security Center of Excellence, 2006).

There is a considerable body of literature about the activities that the ISRM team undertakes with collaboration with relevant stakeholders (Bernard, 2007; Eloff et al., 1993; Spears, 2006; Spears & Barki, 2010). However, the professional and academic literature uses different terminologies to refer to the same process, which creates confusion and may affect the implementation (Eloff et al., 1993) (see Section 5.2.2). In order to provide a clear guidance to the organisation, this section reports the activities undertaken by the ISRM team in high-level and general terminology. These activities are (1) collect risk data, (2) analyse risk data and (3) take appropriate decisions to reduce the risk to acceptable level.

**Practice 4-Activity 1: Collect risk data**

The ISRM team collects data about assets, vulnerabilities, threats, existing controls and risks. Various data collection tools such as interviews, focus groups, surveys, and discussion seminars can be utilised to collect the required data (AS/NZS ISO 31000:2009; Jerman-Blažič, 2008). The team works with stakeholders and encourages them to participate in interviews, surveys and discussion (Bernard, 2007; Microsoft Security Center of Excellence, 2006). Table 5-4 summaries the data that need to be collected.

<table>
<thead>
<tr>
<th>Data type</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td>Anything has a value to the organisation.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Any weakness that can be exploited by an aggressor to make an asset susceptible to change.</td>
</tr>
<tr>
<td>Threats</td>
<td>Causes or events that may negatively impact an asset, represented by loss of confidentiality, integrity, or availability of the asset.</td>
</tr>
<tr>
<td>Existing controls</td>
<td>Description of current controls and their effectiveness across the organisation.</td>
</tr>
<tr>
<td>Consequences</td>
<td>The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.</td>
</tr>
</tbody>
</table>

**Practice 4-Activity 2: Analyse risk data**

Once the data has been obtained, it needs to be analysed. The analysis aims to rank risk according to the likelihood and probabilities. Risk ranking is determined by combining the consequence and likelihood. Likelihood can be defined as the chance or probability of a security
incident or event occurring that would result in particular consequences (Bernard, 2007; Blyth, 2008; Chen & Wen, 2010).

Criteria, that have been developed during the development stage will be used to rank risk in terms of consequences of the risk on the organisation’s information systems and business operations, as well as the likelihood of occurrence (Ronald S Ross & Johnson, 2010; Thapa & Harnesk, 2014). The analysis step will result in a list of risks ranked according to their consequences and likelihood. The list of risks assists the organisation to prioritise which risks need to be treated first.

**Practice 4-Activity 3: Take appropriate decision to reduce risk to acceptable level**

The result from the analysis step will feed into the decision-making step. It will assist the organisation to take an informed decision on what is the best way to treat risks (M. Agrawal, Campoe, & Pierce, 2014; Al-Ahmad & Mohammad, 2013; Ronald S Ross & Johnson, 2010). In other words, the outcome of the analysis helps organisations to select risk treatment options to reduce risks to an acceptable level. Table 5-5 shows ISRM treatment options.

<table>
<thead>
<tr>
<th>ISRM treatment option</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Modification</td>
<td>The level of risk should be managed by introducing, removing or alerting controls so that the residual risk can be reassessed as being acceptable.</td>
</tr>
<tr>
<td>Risk retention</td>
<td>The decision to retain the risk without further action. There is no need for implementing additional controls and the risk can be retained.</td>
</tr>
<tr>
<td>Risk avoidance</td>
<td>The activity or condition that gives rise to the particular risk should be avoided.</td>
</tr>
<tr>
<td>Risk sharing</td>
<td>The risk should be shared with another party that can most effectively manage the particular risk</td>
</tr>
</tbody>
</table>

In addition to the result from the analysis, there are several factors that contribute to the selection of treatment options (Land, Ricks, & Ricks, 2013; Purdy, 2010; Ronald S. Ross, 2011). These factors are the expected cost of the implementation and the benefits from the treatment options. The cost of the implementation includes finance, time, and effort. If the cost of the implementation is higher than the consequences, then the organisation needs to select less expensive treatment options (AS/NZS ISO 31000:2009; HB 174:2003).

The organisation may combine more than one risk treatment option to reduce the likelihood of the risk, thus reducing their consequences (Raz & Hillson, 2005). For example, the organisation
can modify and share risk. Some risk treatments, on the other hand, can effectively address more than one risk.

**ISRM-Practice 5: Communicate the risk assessment result**

Communicating the risk assessment results is a very important practice of the ISRM process (Baskerville, 1991; L. J. Hoffman, 1989; Pattinson & Anderson, 2006). Communication will provide decision-makers and other relevant stakeholders with the necessary information about risks. This risk related information will enable them to take appropriate decisions. Communicating the result consists of two main activities: (1) Document the results of the analysis and treatment plan, and (2) Share the result of the risk assessment process.

**Practice 5-Activity 1: Document the results of the analysis and treatment plan.**

The result of the risk assessment is very important for other information security management practices areas (AS/NZS ISO 31000:2009). It is used as an input for the development stage in ISP management, incident response, and ISTA management (Ahmad, Maynard, et al., 2015). For example, during the development of ISP, the security policy development team must have risk assessment results in hand to be able to develop an effective ISP that addresses the risks faced by the organisation (Eloff et al., 1993; Kadam, 2007). Hence, the first step in communicating the risk assessment results is to document the results and prepare them to be shared with relevant stakeholders. Examples of documenting the risk assessment result is to create risk assessment reports and use dashboard to visualise the results (AS/NZS ISO/IEC 27005:2012; HB 240:2004).

**Practice 5-Activity 2: Share the result of the risk management process**

Once the risk assessment results are well documented, the team should start sharing the results. The results can be shared through an ISTA program. For example, a briefing can be used to share the risk assessment results with decision-makers, and business owners (HB 327:2010). General users can be made aware of the results through an awareness campaign. A copy of the result should be also given to teams of other ISMP areas (policy, ISTA and incident response) to be used as an input to understand the security requirements of the organisations. For more details on how risk assessment results are used in other ISMP areas refer to chapters of each area.
ISRM-Practice 6: Monitor Risk

The organisation’s environment should be monitored constantly and continuously (Raz & Hillson, 2005; Webb et al., 2016). This is because risk is not static; threats, vulnerabilities, likelihood, or consequences may change and as a result of change in the organisational context due to external and/or internal factors (Ronald S Ross & Johnson, 2010). Monitoring of risk enables the organisation to respond to any changes in the risk environment.

Stoneburner et al. (2002) identifies several benefits from risk monitoring: (1) verifying compliance is to ensure that the organisation has implemented the required information security controls to reduce risk to an acceptable level, (2) determining the effectiveness of the security controls put in place to ensure they have been implemented correctly, and are effective in reducing risks, and (3) Identifying any changes in the organisation’s environment (internal and external) that impact the risk. Internal changes include changes in information system by adding new hardware and/or software, which may result in introducing new vulnerabilities (AS/NZS ISO 31000:2009). For instance, upgrading the operating system to new operating system that has less security features.

Organisations should perform ongoing risk assessment to monitor existing risks and identify new risks (AS/NZS ISO/IEC 27005:2012). The organisation should also analyse new or current technologies to identify vulnerabilities and identify the impact on the organisation if those vulnerabilities have been exploited (Whitman & Mattord, 2008).

5.3.3 The Evaluation Stage

The review of both academic and professional literature revealed that there is a gap in the literature in the review and measurement of the effectiveness of the ISRM practices. Existing ISRM standards and guidelines did not focus on evaluating how well ISRM practices are implemented. However, the researcher propose that the evaluation stage should consist of one practice: Review of the ISRM process

ISRM-Practice 7: Review of the ISRM process

AS/NZS ISO 31000:2009 pointed out that risk management activities should be reviewed as part of reviewing and monitoring for risks. AS/NZS ISO 31000:2009 also states that risk management is dynamic, iterative and responsive to change. Therefore, risk management should be reviewed to response to changes as a result of internal and external events. Although risk management standards mentioned the review of ISRM practices, they did not provide sufficient
and clear guidance for organisations on how to review and evaluate their ISRM practices. The review should encompass two activities: (1) review ISRM approach, and (2) Measure the effectiveness of the ISRM practices.

**Practice 7-Activity 1: Review the ISRM approach/criteria**

In the context of the organisation changes, the organisation should review and update its risk management approach. This activity is very important for ensuring accurate and consistent security risk assessment that will lead to effective overall management of risks in the organisations (HB 167: 2006). AS/NZS ISO/IEC 27005:2012 states that “the organisation should regularly verify that the criteria used to measure the risk and its elements are still valid and consistent with business objectives, strategies and policies, and that changes to the business context are taken into consideration adequately during the information security risk management process.” (p.26).

**Practice 7-Activity 2: Measure the effectiveness of ISRM practices.**

The review aims to determine the effectiveness of existing activities (especially risk assessment) (AS/NZS ISO/IEC 27005:2012). The organisation should make sure that the information security risk management process and related activities remain appropriate in the present circumstances and are followed. One possible way to measure the effectiveness of risk management activities is to review recent incident response reports to use lessons from the incident response process as an indication of the accuracy of the risk assessment and to learn about new threats and likelihood and consequences (Ahmad, Maynard, et al., 2015). Another way to measure the effectiveness is to conduct an internal audit to determine whether the organisation’s ISRM activities are undertaken according to the standards and guideline which the organisation adopts.

The next section validates the proposed framework by conducting a series of expert interviews. The empirical data from the interviews will aid in the validation and refinement of the framework and explain how risk management is practised in organisations.

**5.4 Data analysis and findings**

As described in Section 3.5.1 semi-structured interviews were conducted to refine and validate the preliminary framework. A total of thirty-four information security experts were interviewed in this research project (See Table 3-1). Six interviews were mainly conducted to validate the
framework of ISRM practices while the remaining twenty-eight interviews that focused on other areas of ISMP also mentioned the risk management practices but not in detail.

The data obtained from the interviews was analysed as outlined in Section 3.6. Table 5-6 provides details of the ISRM practices that have been identified from the coding and analysis process and the number of participants who supported the practices from the area focused interviews and interviews on other ISMP areas.

Table 5-6 ISRM practices and number of participants that support these practices

<table>
<thead>
<tr>
<th>Stage</th>
<th>Practice</th>
<th>Focused interviews (N1=6)</th>
<th>Interviews of other areas (N2=28)</th>
<th>Total interviews supported the practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Establish risk management context</td>
<td>6</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Establish security risk management team</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Implement &amp; maintain</td>
<td>Facilitate the risk assessment</td>
<td>6</td>
<td>16</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Communicate risk assessment results</td>
<td>6</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Monitor Risk</td>
<td>6</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>Evaluate</td>
<td>Review risk management process</td>
<td>4</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

The remainder of this section presents the key findings and evidence from the empirical study. Supporting quotes will be from the six interviews that focused on ISRM.

5.4.1 The development stage

This section presents participants’ responses to questions related to practices and activities they undertake in order to plan and prepare for ISRM practices. Interviewees reported one key practice undertaken as part of the development stage of the ISRM: Establish risk management context.

**ISRM-Practice1: Establish risk management context**

As discussed in Section 5.2.1 establishing the ISRM context is understanding the environment in which the organisation operates. ‘Establish risk management context’ practice was supported by all six interviewees that focused on ISRM practices. It was also mentioned by five interviewees who discussed other ISMP areas. All six interviewees considered establishing the ISRM context as a planning and preparing practice that organisations undertake prior to conducting a risk assessment practice.
Within the scope of what the literature describes as ‘risk management context’, the participants identified a range of key activities that typically take place. These key activities include (1) Define goals and objectives of the process, (2) Define scope and boundaries of the process, (3) Develop an ISRM approach, and (4) Identify relevant stakeholders.

The following subsections discuss these key activities.

**Practice1-Activity1: Define goals and objectives of the process**

It was agreed amongst all interviewees that the goals and objectives of the process should be defined before the start of the process as part of the ‘Establish risk management context’ practice.

> “Determining why the risk assessment is being performed is almost more important than performing the risk management. So we define the goals and objectives of the process.” P8_Mng_Risk

The goals and objectives of the process can be determined by talking to the relevant stakeholders in the organisation. P10_Mng_Risk, who works as a consultant stated that,

> “we talked to the relevant stakeholders (i.e., management, senior management and managers of particular areas). You want to know what their objectives are and what their concerns are”.

The interviewees highlighted the importance of define goals and objectives in the development stage and stated that setting goals and objectives is extremely useful to check at the end of ISRM process whether the process goals and objectives have been achieved and implement corrective measure to meet the target.

**Practice1-Activity2: Define scope and boundaries of the process**

All six interviewees reported that they define the scope and boundaries of the risk assessment process, the experts stated that it is an essential part of the establishing ISRM context:

> “I'll answer this question from a consulting point of view rather than a person internal to an organisation because there's quite an important process, which is defining the scope and defining what you're gonna write in the proposal, for instance, in order to do risk assessment. We have to define that scope very clearly, very early on in the process.” P8_Mng_Risk

> “Absolutely! So we all generally work within the ISO 27005 framework which requires a scope of what you are assessing.” P10_Mng_Risk

P8_Mng_Risk contended that external and internal factors that may affect risks within the specified scope should be considered during the risk assessment proces of that scope.
“... so although your scope might be just to look at those vulnerabilities, you have to expand. You’re thinking outside of the scope to go, “Well, what else is influencing the vulnerabilities” for instance, and then finding what is it that influences risk.””

**Practice1-Activity3: Develop information security risk management approach**

All participants reported that one of the key activities they undertake as part of establishing the context is to develop an ISRM approach.

“We actually have a risk management document which defines how we define what risk is, categories of risk, the layers of risk, etc.”

“The role of the risk management approach is to assist with how risks should be determined, how they should be documented, how they should be inputted into the portal and the different categories that are adopted as well. That kind of sets the standard.”

All Interviewees stated that the ISRM approach is crucial for guiding and assisting the organisation in identifying assets, threats, and risk rating, and determining likelihood.

“That framework guides us on the calculations for likelihood, the calculations of consequence, the calculations for residual risk when we need to have treatments, who can accept it.”

The interviewees stated that developing the security management approach enables the organisations to have a consistent ISRM process across the organisations and therefore, results of the process can be integrated and compared to provide the executives with accurate information about business risks.

**Practice1-Activity4: Identify relevant stakeholders**

It was agreed amongst all six interviewees that stakeholders play an essential role in the ISRM process. Therefore, participants stated that one of the key activities performed as part of establishing the ISRM context is to identify relevant stakeholders.

“Identifying the stakeholder's is really important and you work with those stakeholders.”

“The risk assessment should be taking place after those key stakeholders are identified and the key business requirements are identified.”

Talking with business stakeholders is very important as they provide a good understanding of the business process:

“business process is really, really important because it has a key input into a risk assessment. You know, it's no good if you're doing a risk assessment, you need that business process to be not only the background to the risk assessment, but also is part of the risk assessment.”
Examples of stakeholders were given by P8_Mng_Risk, P9_Mng_Risk, and P6_Mng_Risk, and include business owners, IT and security teams, senior management, managers of particular areas, and general managers of operations, marketing, and communications.

“When we look at risk within the brands, we do engage with each of the different brand management teams (executives within the brands) to talk about those risks and impact to them.” P6_Mng_Risk

**ISRM-Practice2: Establish risk management team**

While only three out of six participants mentioned the ‘establish risk management team’ practice, during the discussion the participants reported that the responsibility of ISRM process should be delegated or manage by personnel from the information security department. Although some organisations may not call it a team because one or two persons undertake this responsibility, it would be considered as part of this practice.

There are two key activities that are regarded as part of this practice. These key activities are: (1) Define roles and responsibilities, and (2) Schedule risk assessment training for relevant stakeholders.

**Practice2-Activity1: Define roles and responsibilities**

All participants agreed that ISRM was conducted as a team-based exercise. For example, P7_Mng_Risk stated:

“It tends [ISRM] to be a collaboration with different people from different departments.”

In small and medium-sized organisations, a member of the security team, usually the security manager, works as a facilitator of the risk assessment process and collaborates with other stakeholders (i.e., business owners) to assist them to identify assets, risks, and ratings of the risks. There are other risk committees and risk managers; however, they are responsible for managing all risks not just information security risks.

Security consultants may also be brought to some organisations to assist them to conduct ISRM process. In this case the external person (e.g., security consultant) should receive full support and access to stakeholders and documents to establish a thorough understanding of the organisation context and perform the ISRM process in optimal manner.

The idea of a risk management team dedicated to the ISRM process was not supported by the experts. However, when asked whether he has seen an organisation that has a dedicated ISRM team, P8_Mng_Risk pointed out that such teams do exist in exceptional circumstances:
“Yes. Yeah. I'm mainly thinking about banks and some of the larger organisations within Australia, they have had information security risk assessment teams.”  
*P8_Mng_Risk*

P6_Mng_Risk, P8_Mng_Risk, and P12_Cons_Risk provided examples of roles and responsibilities around the ISRM process. These include liaising between the information security team and the rest of the business, business assurance manager, and information security risk specialist.

It is important to note that organisations have risk committees, located under operational risk. These risk committees are responsible for reviewing and monitoring all risks in the organisations, not just information security risks.

**Practice2-Activity2: Schedule risk assessment training for relevant stakeholders**

The participants stated that in many circumstances, when security managers or security consultants take the role of facilitating the ISRM process, they would have the required skills and knowledge to undertake such role. Therefore, participants indicate that there is no specific training for the ISRM process. However, some sort of training for stakeholders (i.e., business owners and executives) may take place during meetings and discussions with the ISRM process facilitator (i.e. security manager or security consultant).

“Almost every quarter [there are] training and updates. And you need to have somebody that actually can do some sort of analysis and deep dive periodically into the information that’s being prepared to make sure that if things are being misclassified, they’re picked up early and you can go back and rectify that either through additional training or clarification.”  
*P9_Mng_Risk*

The roles and responsibilities of the stakeholders that are involved in the ISRM process are considered to be one of key inputs to the needs assessment for information security training and awareness (ISTA). For more details see Chapter 7.

### 5.4.2 The Implementation & Maintenance Stage

This section presents data relating to practices undertaken to implement the ISRM process. Interviewees identified three practices as part of this stage: (1) facilitate risk assessment, (2) communicate the result of risk assessment, and (3) monitor risks.
ISRM-Practice3: Facilitate the risk assessment

All six interviewees agreed that ‘facilitate the risk assessment’ is a key managerial practice in organisations undertake as part of the ISRM process. While sixteen interviewees from the remaining twenty-eight interviewees mentioned this practice.

All six interviewees reported three key activities preformed as part of this practice: (1) collect risk data, (2) analyse risk data, and (3) provide recommendations to reduce risk to an acceptable level.

Practice3-Activity1: Collect risk data.

In this activity a security manager or a consultant conducts interviews and/or group discussions with stakeholders to collect data about assets, threats, etc.

“We will have a workshop with 20 people. For instance, often, workshops can be around business continuity, so, you’ll have a workshop available, what are those, you know, organisations in terms of continuity of operations and what are those threats that affect that continuity of operations, and you know, what are the likelihoods of those threats to occur? So, we tend to do that in your workshop.” P8_Mng_Risk

“I see risk assessment as very much pulling information out of the organisation, usually through interviews with people, and then coming out with a reflection of their own opinions.” P9_Mng_Risk

Prior to the meeting with the stakeholders, a security manager or other external security consultant should do some investigations on the organisation’s current state, audit reports, previous incidents, business processes and objectives, and risk management frameworks.

“But also, prior to a workshop, we tend to go and see the stakeholders, get an idea of what they think the answer is going to be from the workshop, so that when we’re in a workshop situation, we don’t miss out on some of the threats that, you know, may not come from the collective, it would come from individuals, mostly individuals.” P6_Mng_Risk

Data that need to be collected through investigation of the organisation, workshops, and interviews with stakeholders include assets, threats, risks, likelihood, consequences, and existing controls:

“... identify assets, identify threats, identify vulnerabilities and then you do impact and likelihood” P8_Mng_Risk

P8_Mng_Risk, P9_Mng_Risk, and P12_Cons_Risk suggested several strategies for obtaining high-quality data, such as talking to multiple stakeholders, asking people for evidence or support for their statement, doing prior research and creating scenarios,
“I think the key part of the process is to talk to as many stakeholders as much as possible. The quality of the output is directly relational to the quality of the input, so you talk to more people you get better results.” P10_Mng_Risk

**Practice3-Activity2: Analyse risk data**

This activity may take place in parallel with the previous activity of data collection and discussion with stakeholders through interviews and workshops. This activity includes trying to understand the data collected from stakeholders and assisting them to rate risks by applying the organisation’s risk management criteria.

“We try make sense of it, we also try and combine things a little bit so that.” P8_Mng_Risk

“We try and combine things together where it's appropriate to do so, of course, instead of raising five risks when one will do, we'll try to raise one risk, but we'll, you know, identify the things that led us to identify that risk.” P6_Mng_Risk

“We also ask about what an acceptable level of risk is. So, again, depending on the engagement, so it might be acceptable to have a medium risk in a certain area, you know, because, well, you know, the businesses are happy to accept that level of risk. So, when we're looking at inherent risk and residual risk, you know, we're looking at, you know, residual -- current residual risk and then, you know, planned target set residual risk. Well, if you don't have an identification of what is an acceptable level of residual risk, then you might be suggesting controls that actually, the business feel they don't require because they think that the level of risk is acceptable already.” P10_Mng_Risk

**Practice3-Activity3: Provide recommendation to (treat) reduce risk to an acceptable level**

All six interviewees asserted that after doing the risk assessment, they provide recommendations on how risk can be treated or reduced to an acceptable level for the organisation.

“Based on the risk assessment, I will identify what controls you can put in place to reduce that risk” P11_Cons_Risk

“Again, as I say, depending on the engagement, we will come out with a level of risk. We will also work out what is an acceptable level of risk, by again asking the stakeholders and then making some control suggestions to mitigate the risk if it's too high.” P8_Mng_Risk

Interviewees stated that recommended controls can vary from implementing technological controls to managerial controls. In addition, the decision whether to implement a control or not is the responsibility of the risk owner. They understand the acceptable level of risk for their organisation and they take the decision on what they are willing to spend to mitigate a particular risk or accept it.
If we implement these controls, it will reduce the risk to an acceptable level, so it is left to the business owner to say, okay, yes let’s implement the control or no, I accept the risk. It depends on the specific situation.” P11_Cons_Risk

Therefore, a high level of security awareness is required for the risk owner to be able to take the right decision about treatment options they should select to protect their information resources.

**ISRM-Practice4: Communicate the result of risk assessment**

As explained in 5.3.2, the result of the risk assessment is extremely important for other ISMP areas, such as security policy, information security training and awareness, and incident response. The result of the risk assessment is used as an input for the aforementioned areas. As part of the ‘communicate the result of risk assessment’ practice, interviewees reported two key activities: (1) document risk assessment process, and (2) share the result of the risk assessment with relevant stakeholders.

**Practice4-Activity1: Document risk assessment process**

This activity involves documenting the results of the risk assessment process. One way of documenting the risk assessment result is to develop a report that outline information about risks and their factors.

“We fundamentally what you need to do is have a really strong system for documenting all the risks. We produce a quarterly report that goes to the board as opposed to something that could be monitored in real time.” P7_Mng_Risk

“We will do a final report then allow people a chance to read it, and then run a presentation for the role of people. And that'll be, you know, usually the stakeholders identified upfront. Maybe not all of the stakeholders even, sometimes representative.” P8_Mng_Risk

P10_Mng_Risk stated that adopting multiple forms and presentation styles in the risk management report is essential for communicate the risk to different audience.

“We have a number of report templates. Often report templates will be suited for multiple audiences so there will be executive summary area, the heat maps then spider maps and whatever particular graphs are the flavour of the day, and then we will have very detailed tables for the practitioners and the people on the ground.” P10_Mng_Risk

**Practice4-Activity2: Share the result of the risk assessment with relevant stakeholders**

Once the results of the risk assessment are documented and usually a final report is developed, it is necessary to be shared with relevant stakeholders. Participants suggested that results could be communicated via conducting workshops, presentation.
“So basically, we will do it. We will involve them [key stakeholders] in the process but, ultimately, we will put the risk assessment up and we will give them a draft version of it and allow them to provide commentary and this is commentary that they provide or cooperate that into the report and often sometimes light discussion but then will later. Then the final format will only be reported or a report and presentation and all that depends on what the client wants.” P11_Cons_Risk

P6_Mng_Risk, 7_Mng_Risk, and P12_Cons_Risk reported that a ISTA program is developed to communicate risks to employees. For more details on the ISTA management practices see Chapter 7

**ISRM-Practice5: Monitor Risks**

The literature pointed out that risks and their factors are not static. Therefore, constant monitoring of risks is a very important practice of the ISRM process. Consistent with the literature, all interviewees agreed that identifying risks is not enough and that the status of risks need to be tracked to determine whether these risks are being mitigated, as well as determining whether the risk is increasing or decreasing.

As part of the ‘monitor risks’ practice, interviewees reported two activities: (1) Monitor risk through technological means (Dashboards), and (2) Monitor internal and external factors.

**Practice5-Activity1: Monitor risk through technological means (Dashboards)**

Four participants stated that risks are usually monitored through dashboards where major risks and their factors are visualised and tracked in an ongoing basis.

“Dashboards, usually. So one of the most effective ways of actually putting and monitoring risks for the executive. The dashboard is created that will show the residual risk value, the controls, the key controls that have been tested effectively versus ineffective.” P11_Cons_Risk

P12_Cons_Risk, P7_Mng_Risk, and P9_Mng_Risk stated that organisations have the risk committee led by the chief risk office (CRO). This risk committee conducts periodic meetings to monitor risks by looking at the data presented to them in dashboards and other forms of reports about risks, incidents, and regulatory requirements.

“Well basically it depends on the organisation, most areas will have a risk meeting once a quarter, once annually or once a month and all the people will look over the risk.” P10_Mng_Risk

Although organisations use dashboards to monitor risk, it was obvious from the discussion with the experts that implicit in their understanding was that this is only to do with IT risks and that there are other risks that cannot necessarily be monitored using that technique. However, there
is evidence that monitoring is taking place where there is at least an intent to monitor and that from a technological point of view there are tools but from behaviour point view, there may not be tools.

**Practice5-Activity2: Monitor internal and external factors**

Interviewees reported several factors that affect risks. These factors need to be monitored constantly as part of the ‘Monitor risks’ practice. The first factor is information security incidents. It was reported by all participants that information security incidents can be used as a trigger to revisit the ISRM process by either re-conducting the risk assessment or just updating the risk register and reviewing the control to prevent incident from re-occurring.

"Since it’s incident driven, so basically something significant has changed and then someone will go, this risk needs to be changed who have the risk going or is may raise that the risk rating needs to change.” P11_Cons_Risk

The interviewees responses and comments on the learning from incidents reinforce the literature on the importance of using the experience gained from the incident response process to monitor and review risks. However, it seems that the learning is informal as it will not go beyond updating the risk register (adding new risks or changing the rating of existing ones) and the process and the methodology used in the first place for risk assessment seems not to be revisited as a result of incidents.

The second factor that needs to be monitored is compliance and regulatory requirements. P10_Mng_Risk, P12_Cons_Risk, and P6_Mng_Risk reported that any change in the compliance and regulatory requirements could have an impact on risk status and, therefore, trigger re-conducting the risk assessment process.

"The trigger [for ISRM process] might be either regulatory requirements or it might be a requirement from a board perspective that the board wants to know the current state of the organisation from a risk perspective. That’s what triggers the organisation to reassess every six months or 12 months” P12_Cons_Risk

**5.4.3 The Evaluation Stage**

This section discusses practices relating to the review and evaluation of the ISRM process. As discussed in the literature review section the evaluation of information security risk management has not received much attention from either academic or professional in the literature. The literature focused on the ongoing monitoring and review of security risks and their factors. One practice was identified as part of this stage: Review the ISRM process
ISRM-Practice6: Review the ISRM process

Only four out of six participants supported organisations review the ISRM process practice. In large organisations, especially banks, there are multiple committees where the risk assessment process is checked and reviewed to ensure a good understanding of risk and whether proper process and procedure is followed. Two key activities as part of the review was identified: (1) Review risk management approach, and (2) Measure risk management practice effectiveness.

Practice6-Activity1: Review risk management approach

The participants reported that the review practice of ISRM includes reviewing the organisation’s ISRM approach or methodology to check whether any changes in the organisation context have affected the current approach.

“If you have particular risk methodology that is reflected of the fact that you’re updated every six months or 12 months s.” P10_Mng_Risk

“We might have a small committee type structure formed or a loose work group formed to actually conduct annual risk reviews, see if there are any new risks or whatever within the process.” P6_Mng_Risk

Additionally, P6_Mng_Risk & P12_Cons_Risk stated that if the organisation’s risk management approach is not up-to-date, then the results of the risk assessment will not be accurate and therefore decisions made based on these results, may not protect the organisation information resources.

Practice6-Activity2: Measure risk management practice effectiveness

Although all the participants agreed that it is important to measure the effectiveness the ISRM practices specially risk assessment, in practice only two participants reported that they undertake this practice in their organisations.

“deep insight review may take a particular risk category and explore that across the entire organisation or explore it very deep within the division. The output of that review gets shared with all the different heads within the organisation. It’s also handed over to the audit team. The audit team, if you like, would be the third line of risk defense, where they are kind of keeping the police in check to make sure that they are not being persuaded to cover things up.” P7_Mng_Risk

In the previous quote, the expert stated that his organisation performs periodic review (every six or annually) of their risk management process to ensure that all practices are done following the standards and approach adopted by the organisation. This review is done as part of internal and external audit of the ISRM process.
In regard to the risk assessment, three participants stated that the risk assessment is done in an iterative manner back and forth with the stakeholders, so the review of the process is conducted during the implementation and maintenance stage.

“And you need to have somebody that actually can do some sort of analysis and deep dive periodically into the information that’s being prepared to make sure that if things are being misclassified, they’re picked up early and you can go back and rectify that either through additional training or clarification.” P7_Mng_Risk

While the remaining three participants did not report that they review their risk assessment process. The reason for this could be the size of the organisation and the maturity around the ISRM process.

The participants also reported that they review a recent incident response report to use lessons from incident response process as an indication of the accuracy of the risk assessment and to learn about new threats and likelihood and consequences.

5.4.4 Summary of the findings

This section discusses changes to the proposed framework of ISRM practices as a result of the empirical refinement and validation via semi-structured interviews with information security experts. The empirical data has provided rich understanding of the management process of ISRM in organisations which led to changes in practices and activities in the preliminary framework. The changes range from adding activities, reorganising practices and activities, moving practices from one stage to another. Table 5-7 The refined framework of ISRM practices presents the refined framework of ISRM practices.

In the development stage, several changes were made to practices and activities in this stage as following:

ISRM-Practice1: Establish risk management context: unchanged. In principle, there was strong evidence to support this practice as planning and preparation for the risk assessment process. However, the level of detail around the planning activities varies from one organisation to another, depending on the size and maturity of the organisation and the type of engagement of the information security experts. For example, context establishment is undertaken in a formal and detailed manner when the ISRM process is delegated to external subject matter experts (i.e, information security consultants).

The empirical data supported most of the activities identified from the literature as part of the context establishment. However, two activities were not supported by the empirical data, and
were removed from the framework: identify required resources to conduct the process and identify assumptions and constraints to the process.

There is no justification why the participants did not mention these two activities even though they were outlined in the ISO 27005 standard that their organisations adopted as a guide to the ISRM process. There might be several reasons for not mentioning these activities. First, the activities are not well understood, as there are little details in the literature about them. Second, the experts might undertake these activities; however, they do it as a second nature so they do not refer to it in the way the standard does. Third, the level of granularity might be lower than the key activities they have supported as part of the context establishment.

Table 5-7 The refined framework of ISRM practices

<table>
<thead>
<tr>
<th>Stage &amp; maintain</th>
<th>Practice</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Establish risk management context</td>
<td>Define goals and objectives of the process</td>
</tr>
<tr>
<td></td>
<td>Establish security risk management team</td>
<td>Define scope and boundaries of the process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop security risk management approach/criteria</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify relevant stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Define roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schedule risk assessment training for relevant stakeholders</td>
</tr>
<tr>
<td>Implement &amp;</td>
<td>Facilitate the risk assessment</td>
<td>Collect risk data</td>
</tr>
<tr>
<td>maintain</td>
<td></td>
<td>Analyse risk data</td>
</tr>
<tr>
<td></td>
<td>Communicate risk assessment results</td>
<td>Provide recommendation to reduce risk to acceptable level</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop risk assessment documentation</td>
</tr>
<tr>
<td>Evaluate</td>
<td>Monitor Risk</td>
<td>Share risk assessment documentation with relevant stakeholders</td>
</tr>
<tr>
<td></td>
<td>Review risk management process</td>
<td>Implement technological means such as Dashboards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitor internal and external factors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update risk management approach/criteria</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Measure risk management practice effectiveness</td>
</tr>
</tbody>
</table>

Other key activities within this practice remain unchanged: define goals and objectives of the process, define scope and boundaries of the process and identify relevant stakeholders for security risk management.

ISRM-Practice2: Establish security risk management team; unchanged. The concept of having a dedicated ISRM team was not supported by the data as most organisations delegate the coordination and facilitation of the risk management activities to a security manager, a CISO, or an external security consultant. In special circumstances, there might be a group of personnel who manage the general risks in the organisations. For example, in banks, there are different committees and risk lines who manages operational risks to the organisations, including...
information security risks and other types of risks. Therefore, based on the evidence, this practice remained unchanged. The two key activities that are listed as part of this practice define roles and responsibilities and schedule training session for stakeholders also remained unchanged.

*Develop security risk management approach:* change the level. The level of this practice changed as more understanding was gained from the data. The level was reduced to an activity undertaken as part of context establishment.

Practices and activities within the implementation and maintenance stage have undergone many changes:

*Conduct the risk assessment:* changed. The data showed that the managerial practice that represents what is happening in organisations is ‘Facilitate the risk assessment’. Therefore, this practice was changed accordingly.

The two key activities: *Collect risk data* and *Analyse risk obtained data* did not change. whereas *Take appropriate decision to reduce risk to acceptable level* required change. The experts indicated that the decision to implement controls to treat risks is taken by stakeholders and they only provide recommendations to the relevant stakeholders. Therefore, the activity was changed to: *provide recommendation to reduce risk to acceptable level.*

Monitor Risks. Two activities needed to be added to the practice of *Monitor risks.* The empirical data showed that there are two activities that are undertaken to monitor risk: *Monitor risk through technological means (dashboards)* and *Monitor internal and external factors.*

The focus of monitoring was on technological risks and the effectiveness of the implemented controls to mitigate risks. Non-technological risks, such as risks relating to employees’ behaviour were not monitored. There are two main reasons for these actions. First, the view of information security is narrow and limited as information security is perceived from technological perspective rather than a more holistic perspective. Second, the complexity of human behaviour means it is difficult to monitor risks relating to human behaviours.

In addition, the experts reported factors that need to be monitored as part of *Monitor Risks* practice: information security incidents and compliance and regulatory requirements.

In terms of the evaluation stage, although there was no strong evidence to back the practices proposed by the researcher based on the review and analysis of the literature, the participants reported that ISRM approach on the organisation is reviewed and updated periodically. Further,
the participants indicated that internal and external audits are conducted to review the process of risk management. However, this check mainly aims to validate whether the correct procedures for risk management are followed, as opposed to measuring the effectiveness of the risk management practices. The practice ‘conduct periodic review of ISRM process’ therefore remain unchanged. The activities ‘Review risk management approach’ and ‘Measure the effectiveness of the ISRM practices’ did not change.

5.5 Final validation
As explained in Section 3.5.2, an email was sent to each of the six focused interview participants who were interviewed in the first empirical study, to provide feedback on the framework and comments on whether the practices and key activities are comprehensive. Only four participants responded to the email with their comments and feedback on the framework.

Overall, all four participants answered ‘Yes’ to the question ‘Do you think that the framework covers key activities done in organisation in regard to managing their risks?’ they commented that,

“The framework seems to mirror how I experience and progress risk assessments to a greater extent. When compared to the risk management frameworks used in the banking sector this model has captured a great end to end view of a risk cycle” P7_Mng_Risk.

“This risk management practise framework is in line with ISO 31000” P10_Mng_Risk

“This framework represents all key activities we do to conduct risk management process in my organisation” P11_Cons_Risk

One participant provided two suggestions. The first suggestion is that the evaluation stage should feedback to the development stage

“There is also no encouragement to move from Evaluate stage back into the Develop stage, when this may be required for periodic review or on awareness of major changes to the risks, e.g. new threats or change in the scope of the assessment.” P10_Mng_Risk

The proposed framework recognises that ISRM is an iterative process and that the evaluate stage should feed to the develop stage.

The second suggestion is that “Does the Collect risk data activity include collection of history of previous incidents? This is something that I am beginning to see in practice, especially with risk assessments dealing with external threats” P10_Mng_Risk
The researcher agreed with the participant that incident response information is important to understand the organisation context and it should be reviewed during establishing ISRM context, conducting risk assessment and monitoring the risks and its factors.

Another participant also emphasised the fact that risk owner as one of the stakeholders should be identified and risks should be assigned to them. Risk owners should have a risk treatment plan to determine what is needed to mitigate the risk.

No new activities were identified from the analysis of participants comments and feedback. Therefore, the ISRM practice framework did not change.

5.6 Discussion

The analysis of the empirical data enabled a rich understanding of the managerial practices of ISRM undertaken in organisations. The main contribution of this study is the identification of the set of key activities that are required to manage risks and the extent to which these activities are implemented in organisations. No other key activities were identified. The findings have provided an insight of how these key activities have been institutionalized and how well they have been resourced. Following is discussion of the findings related to ISRM practices.

5.6.1 Establishing the context or planning for risk assessment

As mentioned earlier in the literature section almost all ISRM standards and guidelines stress the importance of planning, and outline several activities that organisations should undertake prior to conducting the risk assessment. The findings of this study are consistent with the literature, they indicate that organisations recognise the importance of planning/context establishment and they perform several activities as part of planning and context development. However, the level of details around planning activities varies from one organisation to another depending on the size and the maturity of the organisation and the type of engagement of security experts. For examples, context establishment is undertaken in a formal and detailed manner when the risk management process is delegated to external subject matter expert (i.e, information security consultants), while it is informal and not well documented in small and less mature organisations. Security consultants usually investigate the context of the organisation and follow the project management approach, which includes activities to plan and prepare for the tasks they were asked to do as part of their engagement. Further, during the discussion with the participants, it was apparent that the main focus was placed on the risk
assessment. The participants spent a great deal of time on describing risk assessment (identifying assets, threats and controls, and determining impact and likelihood, etc.); however, it was very challenging to get them to discuss the planning and evaluation of ISRM process. This could be a reflection of the state of the literature, as a considerable body of the literature was devoted to the risk assessment process.

5.6.2 Structure and position of ISRM in organisations

There are two main observations about the current ISRM practices in organisations. First, it was found that a generalised risk management approach is adopted in large organisations where different lines and groups exist to manage risks. In other words, information security risk is not managed within the IT department or information security department, but is managed by operational risks under the Chief Risk Officer (CRO). In each department/business functions, there is an employee who has a background in information security, technology, and business. This employee coordinates and liaises between the security department and the department he/she is located in and conduct risk assessment. Information security risks is aggregated with other types of risks and ranked according to their impact and consequences on the business.

From a strategic point of view, information security risks may not have a high priority in the general risks list, and consequently, do not receive the desired attention in terms of investment and resource allocation. Further, if there are different risk practices adopted in different areas (e.g., performance risks, security risks, and occupational health and safety), and the context within which the risk is being practiced is different across them, then there is an incongruence between their outcomes, because they are all going to one centralised risk register.

If these different areas all report their risks and they are all getting ranked together, the ranking process then becomes misleading, because the assumptions that are made, the estimation technique used or the approach taken are for each one. Therefore, it is important to use “consistent risk measurement criteria that accurately reflect an organisational view ensuring that decisions about how to mitigate risk will be consistent across multiple information assets and operating or departmental units” (Caralli, 2007, p.894)

The second observation is that in many organisations risk assessment is conducted during the initiation and planning phase of any project to ensure that each project satisfies information security requirements of the organisations or the clients in some cases. For instance, if the organisation is embarking on developing a new website to collect payment from customers, the
project manager must involve personnel from the information security department to conduct risk assessment and identify security requirements. Once this is done, the project manager must accommodate and implement the requirements. Then, the information security personnel will check and verify if the security requirements have been met, and decide whether to approve the project or ask for more review and modifications. The project manager must attain the approval from the security specialist before he/she can proceed. Of course, there will be negotiation and discussion between the project manager and the security specialist about what to adopt from the security recommendations, taking into consideration the allocated budget and resources for the project. These two issues were not described in the literature and were based on the rich understanding from the data provided by the participants. Further investigation about the implication of these observations on ISRM process in organisations can be explored in future research.

5.6.3 Strategies to improve the accuracy of risk assessment

Several studies point out deficiencies in the current practice of risk assessment and suggested ways to improve the process (Shedden, Scheepers, et al., 2011; Shedden, Smith, et al., 2010; Webb et al., 2014). A number of strategies were provided by the participants. First, the participants emphasised the importance of undertaking the activities of establishing the context and argued such activities will increase the effectiveness of the risk assessment, because they lead to a greater understanding of the structure of the organisation, the threats landscape, and stakeholders who will assist in the process (Spears & Barki, 2010).

The second recommendation to increase the effectiveness of risk assessment is the participation and involvement of the stakeholders in the process. Stakeholders are vital to the success of the risk management process as they provide input to the process (Baskerville, 1991; Spears & Barki, 2010). The experts reported that in order to get accurate information, they speak to multiple stakeholders around a particular process because each type of stakeholder will describe what they know and how they understand the process. Then, by combining these different views for the systems and the process, the facilitator will be able to construct a comprehensive view and, therefore, provide more accurate information.

The third strategy is to check and validate the information provided by the stakeholders. This is very important for eliminating bias and misleading information where individuals responsible for a particular process or control may exaggerate the threats to justify his/her request for budget. In the other hand, the risk may be understated to fulfil audit requirements. Therefore, the
facilitator of the process should ask for evidence from the stakeholders to support their statement as well as review relevant document such as previous risk assessment and incident response report.

5.6.4 Review and evaluation to determine the effectiveness of the ISRM practices

The overall evaluation of the risk management process has not received much attention from academics or practitioners (Fenz & Ekelhart, 2011; Webb et al., 2014). The focus was mainly given to the ongoing monitoring of the implementation of technological controls. It was obvious from the data that the overall evaluation of the effectiveness of the ISRM practices is not conducted and that the only activity that is considered as part of the evaluation stage is to review the ISRM approach/criteria. The findings of this study indicate that organisation review and update their risk approach periodically, which is very important for ensuring that the organisation’s ISRM approach relevant and up-to-date. An up-to-date ISRM approach will enable organisations to take consistent decisions during the risk assessment in regard to identifying assets, and threats, as well as calculating impact, likelihood and ranking risks. The failure to update the ISRM approach will produce misleading risk assessment outputs that do not reflect the actual risks to the current context and, therefore, will result in incorrect decisions for controls implementation, which will leave the organisations vulnerable to a hostile risk environment.

Although participants reported that internal and external audits are conducted, there was not enough evidence to show that solid and comprehensive evaluation is undertaken to improve the practices in the ISRM process. This review is mainly driven by regulatory requirements or insurance, where the organisation is required to review their ISRM methodology and re-conduct their risk assessment annually or biannually. In this review, a particular risk category is investigated and explored across the entire organisation or deeply within one division. However, the focus is primarily to check whether this risk has changed and the effectiveness of controls implemented as opposed to reviewing the process of identifying this risk. The findings indicate that there is a gap in the practice in the evaluation of ISRM practices and therefore more studies need to be conducted to address this gap by investigating and exploring the evaluation process.

In terms of learning from incidents to improve the process of risk management, the findings also indicate that incidents play a role in re-conducting risk assessment and reviewing individual risk related to a particular incident. The observations of (Ahmad, Maynard, et al., 2015;
Shedden, Ahmad, & Ruighaver, 2010) on single loop and double loop learning has been further reinforced from the evidence in this study. The research findings provide further understanding and more details, that the single loop learning is actually happening in this form: if the incident occurred because of a risk that was not identified, the expert reported that they would add the risk to the risk register, and if the risk is there, they would change the probability. Double loop learning from incidents was not identified, as the participants did not report that they would check and ask questions around why they did not initially identify the risk and manage it.

5.7 Summary
This chapter presented the development, the refinement of an ISRM practices framework. It started by providing an overview of the literature in ISRM highlighting gaps and deficiencies in the area. Then a framework was developed based on a rigorous and systematic review of the literature. The refinement and validation of the proposed framework was also presented. The chapter ended with discussion of the findings from the empirical data. The next chapter will present the development of the information security policy management framework.
Chapter 6 INFORMATION SECURITY POLICY MANAGEMENT PRACTICES

6.1 Introduction
The previous chapter presented the development and validation of the information security risk management (ISRM) practices framework. This chapter reviews and synthesises the knowledge around the managerial practices of information security policy (ISP). The aim of this chapter is to identify managerial practices of ISP and develop a comprehensive framework based on the literature and then validate the information security policy management framework.

This chapter is organised as follows. Section 6.2 provides an overview of existing ISP literature and highlights the research gaps and deficiencies. Section 6.3 presents the proposed framework for ISP management practices. Section 6.4 presents empirical data from expert interviews that were conducted to refine the proposed framework. Section 6.5 presents the analysis and findings of the final validation of the research framework. Section 6.6 discusses the contribution and implications of the proposed framework of ISP management practices. Section 6.7 provides a summary of the chapter and introduces the next chapter.

6.2 Literature review
In the last two decades, research in information security shifted from having a technological perspective to information security towards a managerial perspective that recognises the importance of implementing ISMPs within areas such as policy, risk management, incident response and ISTA (Fenz et al., 2014).

A number of studies in information security literature have focused on information security policy. Earlier studies in the domain (e.g. Lindup, 1995; Maynard, Ruighaver, & Sandow-Quirk, 2002; Ølnes, 1994; Wood, 1995) focus on the importance of having ISP to protect organisational
information assets. These studies argue that security policy is an essential part of an organisation's information security program.

Subsequent research has focused on the ISP information security policy development lifecycle (e.g. Kadam, 2007; Kenneth J. Knapp, Franklin Morris Jr, Marshall, & Byrd, 2009; Rees, Bandyopadhyay, & Spafford, 2003; Whitman, 2008). These lifecycles guide organisations on how to develop an ISP that is specific to their context.

More recently, research on ISP has focused on more specific aspects of ISP such as the quality of the security policy (e.g. Maynard, 2010; Maynard & Ruighaver, 2007), ethics and policy (Ruighaver et al., 2010), users compliance with the ISP (e.g. Bulgurcu et al., 2010; Chen, Ramamurthy, & Wen, 2012; Hu et al., 2012; Li, Sarathy, Zhang, & Luo, 2014; Pahnila, Siponen, & Mahmood, 2007) and involvement of stakeholders in the development of the policy (e.g. Maynard, 2010; Maynard, Ruighaver, & Ahmad, 2011).

### 6.2.1 Models of ISP development

There are a number of studies on the development and implementation of ISP (Bayuk 1997; Kadam 2007; Knapp et al. 2009; Rees et al. 2003; SANS Institute 2001; Whitman 2008). The majority of these studies present the development of ISP as multi-stage lifecycles. Using a lifecycle approach to develop ISP is very beneficial as it allows good management of the development process and assures managers that all the important activities for the development process are performed (Maynard and Ruighaver 2007; Patrick 2002). Ølnes (1994) stresses the importance of having a methodological approach to developing, implementing and maintaining an ISP. Further, Patrick (2002) argues that the use of an ISP lifecycle approach will ensure a comprehensive development process that encompasses all the required activities for developing an effective ISP. Following is a discussion of existing ISP development lifecycles.

Ølnes (1994) proposed a process for the development of an ISP that consists of three stages: development, implementation, and maintenance. The development stage begins with identifying the security goals of the organisation, listing assets, conducting a risk assessment, and selecting security controls, and the implementation stage involves determining responsibilities for implementing and documenting technological controls. The last stage is maintenance and daily operation, which involves monitoring change in the organisation to make possible changes to information security countermeasures to ensure it remains effective in mitigating risks to the organisation’s information systems.
Although the Ølnes (1994) model was designed to address the development of ISP, it describes a general approach to the development of a security program with more focus on identifying risks and selecting controls to mitigate these risks. The model does not specifically address how a policy document is developed, communicated, enforced and evaluated.

In contrast to the general view of Ølnes (1994), Bayuk (1997) presents an ISP development process that focuses on the development of the policy document. The process consists of several steps: identify assets, establish a team to develop the policy, produce the draft policy, review the draft policy, changes as required, and approve and publish the policy.

Several researchers suggest that the development of an ISP goes beyond the development of the document (Patrick, 2002). Patrick (2002) proposed an ISP development lifecycle, that consists of eleven activities, grouped into four phases.

Hare (2002) and Whitman (2008) proposed ISP lifecycles that consist of stages and activities within each stage. Their policy development lifecycles are similar to Patrick’s (2002) lifecycle; however, Patrick’s (2002) lifecycle has an activity-oriented approach, while Hare’s and Whitman’s development models use the concept of stages and activities within each stage. Hare (2002) utilised the project management approach whereas Whitman (2008) applied the system development lifecycle approach.

Regardless of the name and number of stages/phases proposed by Patrick (2002), Hare (2002) and Whitman (2008), the proposed lifecycles begin with understanding the information security problems in the organisation. They proceed to assembling the team and writing, reviewing, and approving the policy documents. Once the policy is approved, the distributing, communicating, and enforcing of the policy take place. The proposed ISP lifecycles also involve ensuring the policy is current through periodic review and evaluation of the policy.

The proposed ISP lifecycles address the development of ISP covering the most important aspects of ISP management. However, they differ in the level of detail and emphasis on particular aspects of policy development. For example, while Hare (2002) presents the process for developing ISP in a systematic way, he takes a more generic approach, so it lacks details about how the policy will be published (what forms online, HTML, etc.), and how it will be communicated and enforced. In addition, Hare (2002) does not discuss the issue of user compliance with the policy and the importance of user awareness and training for communicating and enforcing the ISP in organisations.
Patrick (2002) proposal of an ISP development lifecycle also has a number of issues. Firstly, there are a few overlapping concepts such as compliance, monitoring and enforcement. These three concepts are presented in the approach as three distinct activities but they all represent the management efforts to ensure that the policy is being adhered to by employees. Secondly, the information security training, and awareness (ISTA) program is required for communicating the policy and for enforcement, but the development of awareness and training program is not part of an ISP lifecycle. Lastly, the literature on ISP differentiates between communicating and disseminating security policy whereas the author presents communication as just distribution of the policy.

However, Whitman’s (2008) policy development lifecycle lacks depth. It provides very little detail about many important activities in the process of developing the ISP, such as communicating and enforcing the policy.

Another example of a policy development lifecycle is the PFIRES model for e-commerce ISP development proposed by (Rees et al., 2003). This model was developed using a combination of the system development lifecycle approach and the new-product development lifecycle. As shown in Figure 6-1, PFIRES consists of four phases: assess, plan, deliver and operate. PFIRES has a formalised feedback loop that enables continual feedback to phases in the development lifecycle.

Figure 6-1 PFIRES Framework proposed by Rees et al. (2003)

Although the PFIRES was proposed to assist organisations to develop and manage ISP, it goes beyond the development of the ISP to the development of a security program in the organisation.
It addresses ISP, risk assessment, technological controls and incident response. In terms of the scope of this research, the PFIRES framework covers several aspects related to the policy management practices. For example, in the assess phase, the policy assessment step is conducted to review existing policies, standards, guidelines and procedures. The plan phase also has a step related to the policy management process that is the policy development step. This step presents a methodological approach to create the policy document, which includes activities such as: identify areas for security policy, draft security policy, review security policy and publish security policy. Although the PFIRES framework does not just focus on the policy development process, the framework provides a good overall picture of how the policy development process can be integrated with other information security management areas (risk management, security training and awareness and incident response).

Kenneth J. Knapp et al. (2009) pointed out the lack of a practice-based model that describes the development of an ISP and consequently, developed an ISP process model. The model is based on interviews with certified information security professionals, and consists of several policy management processes (i.e., policy review, risk assessment, policy development, and policy approval). The feedback loop represents the iteration and ongoing nature of those activities.

The review of both professional and academic literature reveals that considerable research effort and progress has been made on the provision of high-level policy management lifecycles or models for organisations. However, there are a number of deficiencies that reduce their utility to organisations seeking guidance on what managerial practices are involved in implementing ISP. The literature: lacks a holistic view of the policy lifecycle (deficiency 1); lacks consistency in terminology and semantics (deficiency 2); uses varying levels of granularity in describing policy management activities (deficiency 3); and makes it difficult to extricate guidance on policy management from that of other practice areas such as risk management and information security training, and awareness (ISTA) (deficiency 4). Table 6-1 summaries deficiencies of existing policy development models.

The first deficiency is the lack of a holistic view of the policy lifecycle. This can be identified clearly in some of the existing policy development lifecycles. For example, Bayuk (1997) presents a process with a narrow view that focuses on the development of policy documents and does not include any practices related to the implementation and the maintenance of the policy. Bayuk (1997)’s process consists of several steps. It starts by identifying assets and then forming a team to develop the policy. Then the draft policy is produced. The draft policy goes through a
review process leading to approval and publishing. Researchers (e.g. Patrick (2002)) suggest that the development of security policy goes beyond the development of the document. Similar to Bayuk (1997), Ølnes (1994) model of policy development is not holistic in that it does not specifically address how policy document is developed, communicated, enforced and evaluated. A recent paper by Al-Mayahi and Sa’ad (2014) focuses on developing a detailed information security policy, rather than providing guidance on the development process of the policy.

### Table 6-1 Summary of Deficiencies identifies in Existing policy development lifecycles

<table>
<thead>
<tr>
<th>Policy development</th>
<th>Deficiency 1</th>
<th>Deficiency 2</th>
<th>Deficiency 3</th>
<th>Deficiency 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rees et al. (2003)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Patrick (2002)</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Knapp et al. (2009)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Karyda et al. (2005)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kadam (2007)</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Hare (2002)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bayuk (1997)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wood (1995)</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Ølnes (1994)</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Whitman et al. (1999)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Whitman and Mattord (2008)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Lowery (2002)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Al-Mayahi and Sa’ad (2014)</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

The second deficiency is that existing policy development lifecycles lack consistency in terminology and semantics. While (Hare 2002; Karyda et al. 2005; Lowery 2002; Patrick 2002; Whitman 2008) present a more holistic view of the policy development process, there are few overlapping concepts such as compliance, monitoring and enforcement. These three concepts are presented in the approach as three distinct activities, while they represent the management efforts to ensure that the policy is being adhered to by employees. Referring to one concept in three different terms or referring to different activities in one term may cause confusion among security practitioners embarking on the process of policy development.

The third deficiency that has been identified is that existing policy development lifecycles use varying levels of granularity in describing policy management activities. Each of the policy lifecycles differs in the level of detail and emphasis on policy development aspects. For example, Hare (2002) presents the development process of security policy in a systematic way, however, details are lacking about how the policy will be published (what form it will take e.g.
online, HTML) and how it will be communicated and enforced. In addition, Hare (2002) did not discuss the issue of user compliance with the policy and the importance of user awareness and training in communicating and enforcing security policy in organisations. The problem with the depth of content can also be seen in the policy development lifecycles proposed (Bin Muhaya 2010; Klaic and Hadjina 2011; Knapp et al. 2009; Lowery 2002; Whitman 2008; Whitman et al. 1999; Wood 1995). The authors provide scant detail about many important activities in the development process of security policy. For example, the lifecycle developed by Whitman (2008) does not provide guidance on communicating and enforcing the policy. Further, Knapp et al. (2009) proposes a model of policy development that presents the process in a very general manner without providing sufficient descriptions of the policy management practices.

The fourth deficiency is the difficulty to extricate guidance on policy management from that of other practice areas such as risk management and ISTA. This is because models such as that proposed by Ølnes (1994), Rees et al. (2003), Knapp et al. (2009) and Patrick (2002) include practices such as conducting risk assessment, development of security awareness program and selection of technological controls as part of policy development lifecycle. This research acknowledges the importance of having risk assessment as an input the policy development process, as well as the need for security awareness and training to communicate and enforce policy. However, this research argues that conducting risk assessment and developing a security awareness and training program are not part of the security policy lifecycle. In fact, the policy development lifecycles proposed by Ølnes (1994) and Rees et al. (2003) go beyond the development of security policy to the development of a security program in the organisation. They address security policy, risk assessment, technological controls and incident response. Security policy is only part of the overall security program that the model focuses on.

Although existing policy development models and lifecycles collectively provide good advice for policy development, the review of the literature shows evidence of four critical deficiencies that affect organisations seeking to implement security policy. The review also supports Knapp et al. (2009)’s assertion that there is a need for empirical research in the area as the majority of existing policy development lifecycles are conceptual and lacking support from empirical data. Therefore, there is a need to develop a comprehensive, coherent and empirically tested security policy management practices model that addresses the four deficiencies in literature.
6.2.2 Stakeholders Involvement

There is a wide consensus in the literature on the need to involve multiple perspectives in the process of developing ISP (Doherty & Fulford, 2006; Kadam, 2007; Maynard & Ruighaver, 2003; Maynard et al., 2011; Rees et al., 2003; Whitman, Townsend, & Aalberts, 2001). Ølnes (1994) stresses the necessity of engaging the whole organisations in the development process. Examples of main policy stakeholders includes Executive Management, business unit representatives, user community, human resources, ICT specialists and security specialists (Maynard, 2010).

There are many benefits of engaging different stakeholders of the organisation in the ISP management process. Maynard et al. (2011) assert that “having multiple stakeholders involved in ISP development will help to produce a more balanced policy that will be applicable to the diverse stakeholders of the organisation” (p.182). The involvement of different stakeholders has a positive impact on the acceptance of the policy, as employees will feel that they have ownership of information security. This will change their attitude towards information security in the organisation and ultimately have a positive impact on their compliance with the ISP (Maynard et al., 2011; SANS Institute, 2001; Siponen, Mahmood, & Pahnila, 2014; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014).

6.2.3 Compliance

The issue of employees’ compliance with ISP is a key problem for organisations (Ifinedo, 2014; Puhakainen & Siponen, 2010; Symantec Corporation, 2014). Recent security reports suggest that Employees’ noncompliance is the cause of over half of all information security incidents(Symantec Corporation, 2014). Consequently, the issue of compliance with ISP has been the focus of research in the ISP domain (Ifinedo, 2012; Li et al., 2014; Puhakainen & Siponen, 2010; Siponen, Pahnila, & Mahmood, 2007; Vroom & von Solms, 2004). The majority of empirical works in the ISP domain are in compliance.

Several studies have been conducted to understand why employees do not comply with policy, and have explored factors affecting employees’ compliance with ISPs (Abdul Molok, Ahmad, & Chang, 2011a; Hedström, Karlsson, & Kolkowska, 2013; Hu et al., 2012; Siponen et al., 2014; Vance et al., 2012; Wall, Palvia, & Lowry, 2013). These studies used different theories to study the phenomena: general deterrence theory, rational choice theory, situational crime
prevention theory, planned behaviour the protection motivation theory, the theory of reasoned action, and the cognitive evaluation theory.

For example, a recent study by Siponen et al. (2014) applied a combination of three theories namely the protection motivation theory, the theory of reasoned action, and the cognitive evaluation theory to understand factors that influence employees’ adherence to the ISP. The study identified five factors that have a significant impact on employees’ compliance with an ISP (perceived severity of potential threats, perceived vulnerability to potential threats, attitude towards complying with security policy, social norms towards complying with the ISP and intention to comply with security policy).

Similar to other studies on the compliance issue, (Siponen et al., 2014)’s study provides recommendations to aid organisations to achieve better compliance with their ISP. These recommendations include instilling in employees the importance of information security, developing clear ISPs, and providing information security education, training and awareness for employees to assist employees to perform their job in a secure manner.

The literature on the issue of compliance suggests that compliance is closely linked with ISP management practices. In other words, good ISP management practices lead to better compliance with the ISP. Hence, compliance should be taken into consideration during the development, implementation, and evaluation of the ISP in the organisation. Each practice undertaken to manage ISP in the organisation should play a significant role in achieving better compliance with the policy. For instance, (Flowerday & Tuyikeze, 2016; Lopes & Oliveira, 2015) argue that the involvement of relevant stakeholders will have a positive impact on their understanding of the information security problem and therefore, their adherence. Other researchers believe policy should be communicated to employees through an ISTA program to provide employees with the required knowledge and skills to enable them to comply with the ISP (Hu et al., 2012; Safa, von Solms, & Furnell, 2015). In addition, several studies suggest that consistent enforcement of the ISPs is crucial to make employees comply with them (Chen et al., 2012; Sommestad et al., 2014).

6.2.4 Information security policy quality

Assessing the quality of the policy is an important issue that has to be addressed in the management of the ISP. Maynard and Ruighaver (2003) evaluated existing policy development methods, and stated that existing policy development methods “briefly describe the development
of the policy as a process that goes through continual re-development, yet neglect to specify how it is determined what needs to be updated, added or removed from the policy” (p.357). Consequently, there is a lack of guidance on how to assess an ISP and who should be involved in the assessment process.

Subsequently, Maynard (2010) proposed a policy quality framework based on software development quality and data model quality. The model consists of factors that can be used to determine the quality of the ISP within an organisation (Maynard & Ruighaver, 2006). Further the authors explored the perspectives of different stakeholders on the quality of an ISP and the involvement of these stakeholders in the quality assessment process (Maynard & Ruighaver, 2007).

Implementing good ISP management practices should result in improving the quality of the policy. Hence, this research aims to provide organisations with guidance on how to manage ISP effectively and develop high quality policies.

6.3 Information Security Policy Management Practice framework

As described in Section 4.3.2, a comprehensive and rigorous review of the information security policy literature was conducted. The following search terms: ‘information security policy’, ‘information security policy development’, ‘security policy management’, ‘policy development lifecycle’ were used to search in various databases and search engines. For more details about the search results and analysis process see Section 4.3.2

The overall understanding that emerged from the comprehensive review and coding process resulted in the development of a framework of information security policy management practices. This section discusses the proposed framework. Table 6-2 depicts the framework that consists of three main stages: the Development stage, the Implementation & Maintenance stage, and the Evaluation stage (see Section 4.3.3). Each stage consists of a number practices, each having a number of key activities.
6.3.1 The Development stage

The development stage of the process of managing ISP represents all the practices associated with the development of the ISP. There are three practices within the development stage: (1) establish information security policy development team, (2) determine the security needs of the organisation, and (3) compile the security policy document

**Policy-Practice 1: Establish information security policy development team**

The first practice that information security managers in organisations must undertake in the process of developing an ISP is to establish the policy development team (Doherty, Anastasakis, & Fulford, 2011; SANS Institute, 2001; Whitman, 2008). There are two main activities in this practice: (1) identify key stakeholders and (2) define roles and responsibilities.

**Practice 1-Activity 1: Identify key stakeholders**

The involvement of relevant stakeholders in the ISP development process is a success factor for security policy in the stages of development, implementation and evaluation (Flowerday & Tuyikeze, 2016; Safa et al., 2015). Therefore, a team of representative stakeholders from across
the organisation at all levels is assembled (Kenneth J. Knapp et al., 2009; Rees et al., 2003). Representative stakeholders in the organisation may include technical personnel, process owners, decision makers, managers, the legal department, the human resource department, users, and other function area personnel affected by the new policy (Maynard et al. 2011; Ølnes 1994; Wood 1995). The scope of the developed policy is an important factor for determining who should be involved in the development process (Patrick 2002). For example, an ISP developed for a specific department within the organisation may involve less people in the development process than a policy developed for the entire organisation.

**Practice 1-Activity 2: Define roles and responsibilities**

It is important to clearly define the roles and responsibilities of development team members to avoid delays in the development process due to interpersonal challenges and political objections that may occur (SANS Institute 2001; Whitman and Mattord 2010; Wood 1995). Maynard (2010) asserts that while many authors emphasise the importance of involving different stakeholders in the development process; the roles of these stakeholders remain unclear. He also points out that authors simply mention the name of the stakeholder that needs to be involved in the development process without specifying what this group of people should do in the process. Therefore, Maynard (2010) discusses the roles of each stakeholder involved in the process of developing the information security policy. For example, the security specialist undertakes responsibilities such as liaise with the risk assessment team, lead the development, implementation and review process (Maynard 2010). Another example of roles and their responsibilities regarding the policy management process is executive management who is responsible for the overall governance of the policy including oversight and approval of the policy (Maynard,2010).

**Policy-Practice 2: Determine the security needs of the organisation**

After establishing the policy development team, the organisation should determine its security needs (Rees et al. 2003; SANS Institute 2001; Whitman and Mattord 2010). A comprehensive understanding of the current situation of the organisation, as well as sufficient understanding of the organisation’s security goals and objectives, is required (Ølnes 1994; Palmer et al. 2001; Stahl et al. 2012). This can be done by conducting a thorough investigation of the problem facing the organisation (Whitman 2008). Determining the security needs of the organisation consists of two activities: (1) identify security requirements and (2) assess the organisation’s current policies and procedures.
Practice 2-Activity 1: Identify security requirements

Due to the fact that organisations have different security needs, organisations have different security requirements and objectives (Karyda et al. 2005; Ølnes 1994; Wood 1995). Baskerville and Siponen (2002) argue that it is important to have a good understanding of the organisation’s security requirements when developing an ISP. Therefore, the organisation should identify its security requirements, including the level of security that the organisation aims to achieve. Security requirements should specify the requirements of the organisation for addressing security risks that have been identified through risk assessment, in order to fulfil its security needs and achieve its business objectives.

The result of the risk assessment is an input to identify security requirements, therefore, some authors include risk assessment as a practice in their ISP lifecycles (Bayuk 1997; Gaunt 1998; Rees et al. 2003). However, although the result of risk assessment is a prerequisite for identifying the security requirements, assessing risk should be part of information security risk management, rather than policy development. Wood (1995) stated “ideally, a policies development effort should be initiated after the performance of a comprehensive information security risk assessment” (p.673)

Practice 2-Activity 2: Assess the organisation’s current policies and procedures

Assessing currently implemented ISP and procedures has several benefits. First, it aids the security development team in understanding the current status of existing policy and procedures (Doherty and Fulford 2006; Palmer et al. 2001; Rees et al. 2003; Whitman 2008), which is important, as it allows the organisation to identify gaps in current policy and to determine whether the existing policy will help the organisation to address risks by meeting its information security requirements. The organisation can then identify areas that need to be addressed by the new policy. Second, assessing existing policies and procedures will ensure that new policies conform to existing policy standards (SANS Institute 2001), which will increase the chance of successful implementation of the updated policies in the organisation (Peltier 2013). Third, the assessment process helps gather key materials, such as existing policy and procedures documents, that will be used by the development team as key reference (Patrick 2002; Whitman et al. 2001).

Policy-Practice 3: Compile the security policy document

Compiling the ISP document is the last practice in the development phase of an ISP. The policy document should state management’s commitment and direction, and set out the organisation's
approach to managing information security (ISO/IEC27002 2006). Maynard and Ruighaver (2003) argue the importance of documenting the information security policy development process to both justify the development process itself and aid in the evaluation of any existing policy.

Compiling the policy document consists of a number of activities (1) selecting policy components, (2) draft security policy and (3) review draft policy document (Hare 2002; Patrick 2002; Whitman 2008).

**Practice 3-Activity 1: Select policy components**
The policy development team selects policy items that will address the information security needs of the organisation (Lowery 2002; Rees et al. 2003; Wood 2005). Policy items may address access control, Internet usage, the use of mobile devices and portable storage devices, and so forth. For example, access control items should discuss authorised access to the systems, ways to control access (passwords and/or biometrics), and consequences of unauthorised access (Whitman et al. 1999; Wood 2005).

**Practice 3-Activity 2: Draft security policy**
The policy development team should appoint one of its members to write the policy (Anderson Consulting 2000). The rest of the team should provide guidance on the context and content of the policy. Höne and Eloff (2002b) explore the factors that make an ISP an effective control in protecting organisational information assets. They report on characteristics that should be considered when writing ISP. These characteristics are concerned with the length and writing style. An ISP document should be short because if it is too long, the users will not read it. Many authors (e.g. Stahl et al. 2012; Whitman 2008; Wood 1995) highlight the importance of using appropriate language when writing ISP. They suggest that the ISP should be written in clear, concise, and easy to understand language. Table 6-3 provides a summary of sections and attributes that should be included in the policy documents (Anderson Consulting, 2000; Whitman, Townsend, & Aalberts, 1999).

In his study of the quality of information security policy, Maynard (2010) identified usability as a quality dimension of security policy. Usability is defined as “the effort required for stakeholders to create, use and update the information security policy” (p.128). Usability has four characteristics: Understandability, Learnability, Operability and Attractiveness. In relation to this activity, two characteristics of the usability dimension should be considered while writing
the policy documents. These two characteristics: understandability and attractiveness. Understandability means that the policy document should be written in a way that should be easy to be understood by stakeholders. While attractiveness is ensuring that the policy document is well organised and formatted to be attractive to the stakeholders (Maynard, 2010).

Table 6-3 Summary of sections and attributes of security policy documents.

<table>
<thead>
<tr>
<th>Section of Policy document</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Provided by security organisation following a standard format</td>
</tr>
<tr>
<td>Version</td>
<td>Version number of the document so it can be version controlled</td>
</tr>
<tr>
<td>Purpose</td>
<td>Aims of the policy and problems the policy will resolve</td>
</tr>
<tr>
<td>Scope and audience</td>
<td>The intended audience and the environments to which it applies</td>
</tr>
<tr>
<td>Overview</td>
<td>A briefly explanation of relevant security issues including specific threats and vulnerabilities to consider</td>
</tr>
<tr>
<td>Roles and responsibilities</td>
<td>Define who is responsible for what action</td>
</tr>
<tr>
<td>Content</td>
<td>Identify and explain all relevant information</td>
</tr>
<tr>
<td>Reporting</td>
<td>Information for reporting all security violations and security incidents</td>
</tr>
<tr>
<td>Related documents</td>
<td>List any related forms and link if possible.</td>
</tr>
<tr>
<td>Authors and history</td>
<td>A record of the original author, authors of revisions, and synopsis of each revision change.</td>
</tr>
</tbody>
</table>

Practice 3-Activity 3: Review draft policy document

Once the first draft of the policy is created, it should be presented to relevant stakeholders to review and provide feedback about quality, usability, and acceptance of the policy (Kadam 2007; Lindup 1995; Whitman 2008). Feedback on policy should be sent to the author to update the policy. Policy writing, and revision are an iterative process (Rees et al. 2003). In other words, the draft may progress through many revisions until the final policy is produced. The final policy will be sent to top management for final approval. Then it will be published and ready to be implemented (Whitman 2008).

6.3.2 The Implementation and Maintenance Stage

The implementation and maintenance stage is the second stage of the ISP management process. It is an ongoing process, which consists of several practices. Following is a discussion of ISP management practices within this stage.
**Policy-Practice 4: Distribute policy**

The practice of distributing the policy is to ensure that all stakeholders in the organisation, including users and managers, have access to the policy document (Höne and Eloff 2002a). Effective dissemination of the policy to the individuals affected by the policy requires a substantial effort from the organisation in order for it to be done effectively (Whitman 2008). The distribution of the policy involves: (1) Selecting the delivery methods and (2) using the delivery methods to deliver the policy.

**Practice 4-Activity 1: Select policy delivery methods**

There are various ways to distribute the policy in the organisation (Gaunt 1998; Lindup 1995; SANS Institute 2001; Whitman 2008). While some organisations prefer a hardcopy dissemination in which a printed copy of the document is delivered to the employees, others publish the policy electronically through email and the internal and external network (Whitman 2008). No matter what methods the organisation chooses to distribute the policy, it should be available and easy to access (SANS Institute 2001). Therefore, the organisation should select the most appropriate policy delivery methods to ensure that the policy reaches the people it applies to. The selection of the delivery methods depends on the organisation’s environment and the preference of the employees.

**Practice 4-Activity 2: Deliver the policy documents**

After the selection of the delivery methods, the policy should be prepared in the appropriate format, whether it be HTML, PDF or a Word document (Anderson Consulting 2000; Hare 2002). The format is guided by the delivery methods selected and the organisations preferences. Once the appropriate format is prepared the distribution of the policy takes place. Particular attention should be given to the presentation of the policy when delivering it to stakeholders via an organisation’s intranet. This is because the presentation of the policy may have some impact on stakeholder’s perceptions of quality (Maynard, 2010).

**Policy-Practice 5: Communicate policy**

In distributing the policy, the organisation has no guarantee that the individuals who receive the policy will actually read it. Therefore, the organisation must communicate the policy (Rees et al. 2003; SANS Institute 2001; Sommestad et al. 2014). Communicating the policy is an essential practice for its enforcement (Knapp and Ferrante 2012; Siponen et al. 2007; Whitman
et al. 2001). Successful communication of the policy also leads to better compliance from employees (Sommestad et al. 2014).

Communicating the policy is important in assisting the organisation to manage changes in its processes caused by the implementation the new policies (Maynard and Ruighaver 2003). Communicating the policy has three main objectives: to make users aware of the policy, to communicate the reason for implementing the policy, and to make users aware of how it will affect them and what the implications are if they do not comply (Knapp et al. 2009; Maynard and Ruighaver 2003).

There are a number of ways to communicate the policy, including via security education, training and awareness (ISTA) programs (Bauer & Bernroider, 2017; Gjertsen, Gjære, Bartnes, & Flores, 2017). Siponen et al. (2014) emphasise the importance of a ISTA program for teaching the organisation’s employees about their role in maintaining the policy so that the policy becomes ‘as an integral part of their job’. In the same vein, Whitman (2008) stresses the significant role that an awareness program plays in keeping policies fresh in employees’ minds. For example, the ISP can be communicated by conducting training sessions to teach users how to perform the information security procedures that the ISP requires. Another example is to use an awareness campaign to raise people’s awareness about the organisation’s policy. An ISP can also be communicated through a monthly briefing, to ensure that employees not only understand the policy, but also have the necessary skills to adhere to the policy guidelines.

**Policy-Practice 6: Enforce policy**

Enforcing policy is an ongoing activity to ensure that the policy is adhered to (Hare 2002; Lowery 2002). Policy enforcement does not simply involve identifying and penalising violators. Enforcement is a managerial activity that considers the unauthorised act itself, as well as the severity of the offence and the user’s intent (Puhakainen and Siponen 2010).

The literature emphasises the importance of policy enforcement, and that without enforcement, the ISP has no value (Doherty and Fulford 2006; Knapp et al. 2009; Rees et al. 2003; Whitman 2008). The SANS Institute (2001) reports that to mitigate risks to information security the “*policy must be enforced in a strict manner, and noncompliance must be punished*” (p.8). Enforcement and compliance needs to be in place to ensure effective implementation of the ISP (Al-Mayahi and Sa’ad 2014).
In order to enforce policy a number of activities need to be accomplished. First, technological mechanisms need to be implemented. These mechanisms include user administration (adding, deleting and modifying system and application users), evaluating and applying security patches to systems and applications, system and application monitoring for security events, and administering anti-virus applications (Li et al. 2014; Rees et al. 2003). Second, enforcement can be done by conducting a ISTA program to change employees’ behaviour towards adherence to the ISPs (Siponen et al. 2014; Sommestad et al. 2014). Vance et al. (2012) argue that organisations should shift from enforcing policy through the implementation of incentives and sanctions towards creating a shared vision of the ISP. This argument supports the claim made by several authors (e.g. Hassan and Ismail 2012; Lim et al. 2010; Oost and Chew 2012; Ramachandran et al. 2012; Ruighaver et al. 2007) that establishing a security culture will result in better compliance with security policy.

6.3.3 The Evaluation Stage

An effective security policy requires constant review and revision. The Evaluation stage has two main objectives: (1) to determine if the policy still effective and (2) to identify the needs to update policy to incorporate to organisational changes. The process of evaluating the security policy serves as a feedback mechanism providing input for the development of the policy.

Policy-Practice 7: Review information security policy

There is wide agreement in the literature that an ISP needs to be reviewed periodically (Knapp et al. 2009; Maynard and Ruighaver 2003; Rees et al. 2003). The organisational environment, both internal and external, changes constantly, which leads to changes in the information risks that the organisation faces. In order for the ISP to continue to be current, effective and relevant, it needs to be reviewed and updated. To accomplish the review practice two main activities should be carried out: (1) collect feedback from relevant stakeholders about the ISP, and (2) examine security incidents’ reports and new risk assessment

Practice 7-Activity 1: Collect feedback from relevant stakeholders about the ISP

Feedback can be collected from relevant stakeholders (managers, users, etc.) using interviews, and surveys, and other data collection means (Anderson Consulting 2000). The feedback should be analysed to determine the effectiveness of the policy, to monitor compliance and to determine the relevance of the policy. This data collection will help to identify whether the organisation needs to modify the policy and also helps to avoid the risk of having an outdated and irrelevant
ISP which would an ineffective control for mitigating risks (Anderson Consulting 2000; Patrick 2002).

**Practice 7-Activity 2: Examine security incidents’ reports and new risk assessment**
The importance of gathering information security incident data to inform policy development cannot be underestimated. The number and type of incidents can be strong indicators of whether the policy is no longer effective (Bañares-Alcántara 2010; Kadam 2007; SANS Institute 2001). It can help to identify areas in the existing policy that must be updated, added, or removed. In other words, it helps to recommend possible changes in the current policy to ensure that the organisation’s ISP remains an effective control for protecting the organisation from the evolving risk environment.

In terms of when a policy review takes place, several researchers suggest that the review and revision of the policy should be undertaken at least annually (Höne and Eloff 2002a). Others, however suggest that it should occur whenever major changes in information systems of the organisation are made (Palmer et al. 2001; Sommestad et al. 2014; Wood and Lineman 2009). Security incidents may also trigger the process as well (Ahmad et al. 2015; Park et al. 2012).

The management of ISP is an iterative process. Therefore, the review practice provides a valuable feedback on the current policy (the need to change and update the policy) for the development stage in the policy management practices.

**6.4 Data Analysis and Findings**
As described in Section 3.5.1 semi-structured interviews were conducted to refine and validate the preliminary framework. A total of thirty-four information security experts were interviewed in this research project (see Table 3-1). Five interviews were predominately about information security policy management practices while the remaining twenty-nine interviews that focused on other areas of ISMP also mentioned policy. The data obtained from the interviews was analysed as outlined in Section3.6.

Table 6-4 provides details of the information security policy practices that have been identified from the coding and analysis process and the number of participants who supported the practices from the area focused interviews and interviews on other ISMP areas.
Table 6-4 policy management practices and number of participants that support these practices

<table>
<thead>
<tr>
<th>Stage</th>
<th>Practice</th>
<th>Focused interviews (N=5)</th>
<th>Interviews of other areas (N=29)</th>
<th>Total interviews supported the practice.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Establish policy development team</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Determine organisation’s security needs</td>
<td>5</td>
<td>7</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Create security policy document</td>
<td>5</td>
<td>13</td>
<td>18</td>
</tr>
<tr>
<td>Implement &amp; Maintain</td>
<td>Distribute security policy</td>
<td>5</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Communicate the security policy</td>
<td>5</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Enforce the security policy</td>
<td>5</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>Evaluate</td>
<td>Review information security policy</td>
<td>5</td>
<td>16</td>
<td>21</td>
</tr>
</tbody>
</table>

The remainder of this section presents the key findings and evidence from the empirical study. Supporting quotes will be from the five interviews that focused on security policy.

6.4.1 The development stage

This section presents the key findings and evidence related to practices undertaken to develop an ISP. Three main practices were identified by the interviewees as important practices for developing an ISP: (1) establish information security policy development team, (2) determine the security needs of the organisation, and (3) compile security policy document. The following subsections discuss these three practices.

Policy-Practice 1: Establish policy development team

The ISP development team is defined as a group of people responsible for managing the policy development process. All five interviewees agreed that as a part of the management process of ISP, a team should be established in the organisation. Although, this particular practice has been mentioned directly by the remaining 29 interviewees of other ISMP areas, the concept of having responsible security personnel/team for each ISMP areas was supported by all 34 interviewees. Interviewees identified two activities as part of this practice: (1) determine the structure of the security policy team, and (2) define roles and responsibilities for managing security policy.

Practice 1-Activity 1: Determine the structure of the security policy team

All five interviewees stated that the structure of the policy development team varies depending on the organisation’s size and availability of resources. Interviewees reported two common structures in regard to the ‘policy development team’ in organisations: (1) a formal ISP team
that is dedicated to only undertaking practices to manage the ISP in the organisation, and (2) an informal team that consists of members from the organisation’s security team who have other responsibilities besides managing the development process.

“In our organisation we have 2 or 3 people who are responsible for the development process of security policy.” P1_Mng_Policy

“In some organisations they have a defined security team, couple of guys in the team are responsible for writing policies” P3_Cons_Policy

“The process of producing the policy document and the standards itself is run by a team of one or two people” P4_Mng_Policy

P2_Cons_Policy, P3_Cons_Policy, and P5_Cons_Policy also reported that as information security consultants, they have been involved in various organisations where they have been brought in to assist the organisation in the management process for the ISP.

Practice 1-Activity 2: Define roles and responsibilities for managing security policy

All Interviewees stressed the importance of clearly defining the roles and responsibilities of the ISP team’s members. Those who should be involved in managing the ISP include security manager, security policy manager, and chief of information security office.

“Actually there are two people in our organisation who are responsible for policy development, CISO [chief information security officer] and chief risk officer (CRO). So they actually work together to develop information security policy.” P4_Mng_Policy

P5_Cons_Policy commented that the policy development team discusses the role of people who should participate in the development process,

“from policy perspective, we talk about the nature of the role that needs to be involved.” P5_Cons_Policy

Interviewees stated that they have to determine who is doing what in regard to managing the ISP in the organisation. They provided examples of activities, that should be performed, such as identifying security requirements, creating an initial ISP document, communicating with stakeholders to obtain their feedback, etc.

Policy-Practice 2: Determine the organisation’s security needs

In this practice, the team responsible for the development process conducts a gap analysis and investigate the current state of the organisation. This practice has been supported by all five participants, and from the remaining twenty-nine interviewees, seven participants mentioned this practice. Determine the organisation’s security needs includes three main activities: (1)
assess the organisation’s current policies and procedures, (2) identify security requirement and (3) identify key stakeholders.

**Practice 2-Activity 1: Assess organisation’s current policies and procedures**

All five interviewees mentioned that one of the activities, that should be undertaken to determine the organisation’s information security, is to assess exiting policies and procedures. P4_Mng_Policy stated that:

“The first step is to check whether the organisation has a policy in place. If YES! Then we review the existing policy”.

All interviewees reported that an ISP is reviewed periodically, and the result of the review will be used as an input to the development stage. More details on the ISP review practice will be discussed on Section 6.4.3

**Practice 2-Activity 2: Identify security requirements**

It was generally agreed amongst all interviewees that information security requirement should be identified as part of determining the security needs of the organisation. Interviewees provided an in-depth discussion about ways to identify security requirements. Three key inputs for identifying the security requirements were mentioned by the interviewees: information security risk assessment reports, compliance and regulatory requirements, and information security incident reports.

“There are a number of ways to do that [identifying requirements]. Often this can be as a result of a risk assessment, because you need to understand what are the key risks to the organisation.” P1_Mng_Policy

“Another way of doing it can be compliance, so for example, an organisation will seek to apply PCI DSS [The Payment Card Industry Data Security Standard] or ISO 27001 or the protective security policy framework. You'll have a policy that basically maps to the requirement of that particular standard and then you are putting in controls to do that.” P2_Cons_Policy

When asked whether they refer to incident report, both P1_Mng_Policy and P3_Cons_Policy replied “Yes, that’s part of the current state process” He also added that in mature organisations risk assessment and incident report would be a reliable input to identify the security requirements of the organisation.

“if it’s in a mature organisation, you go through their different risk assessment reports, you go through the change management reports, what happens there? The incidents that have happened, lots of different things.”
Additionally, all interviewees mentioned the essential role of stakeholders in assisting the development team, either internal team or external consultant, to identify security requirements as they provide inputs to the process. The following quote indicates that interviews are conducted with stakeholders to help understand the organisation’s business process, strategic priorities and risk appetite.

“In most cases, you build a policy, show it to them and then you see them going all haywire, ‘No, this is not going to work. This is going to be this problem in this one.’ You go through that heated discussion or that whatever you want to call it. Sometimes a good discussion as well but often it’s a heated discussion and then you get to know their inputs, how they function and what their thoughts are about it.” P5_Cons_Policy

Practice 2-Activity 3: Identify key stakeholders
It was agreed amongst all five interviewees that the success of the development process depends on the involvement of relevant stakeholders. Interviewees also argued that if stakeholders were not involved in the process, then there is a risk of developing ineffective policy. P1_Mng_Policy stated:

“I have seen policy that has not been developed by the right people. This results in a policy which is difficult to implement and not properly developed” P1_Mng_Policy

Therefore, interviewees stated that it is important to identify the key stakeholders before starting the ISP development process:

“Before we start the [policy development] process we identify who should be involved and which one is doing what.” P3_Cons_Policy

Three interviewees described the process of identifying stakeholders. They reported that they meet business representatives and discuss with them what policies need to be develop and ask them to assist in identifying the stakeholders who should be involved in the development process. They also provided examples of relevant stakeholders, which include executive level management and middle management.

Policy-Practice 3: Create security policy document
All five participants supported this practice. It was also mentioned by thirteen participants in the interviews of other ISMP areas. The interviewees described the activities undertaken as part of ‘Create the policy document’ practice. These activities include (1) develop the initial security policy document, (2) Develop subsequent security policy, (3) approve the final draft.
Practice 3-Activity 1: Develop the initial security policy document
The policy development team writes the policy and shares it with the relevant stakeholders for review and comment.

“We draft the document because we are a consulting company, so we are brought in to write policies for organisations” P2_Cons_Policy

Participants stated that the policy should be easy to read and understand by stakeholders. Therefore, they recommended that technical language should be avoided in the document.

Practice 3-Activity 2: Develop subsequent security policy.
As previously mentioned that once the initial policy document is created, it will be shared with relevant stakeholders to review the document and provide feedback. The team gives the stakeholders a specific timeline for sending their feedback to the team. Once the feedback is received, several meetings are conducted to discuss the feedback and reach a point of agreement upon certain issues:

“once the policy is created, it is shared with all the relevant stakeholders. We gave them a certain amount of time where they are supposed to review the policy and come out with changes. Then we review their suggestions and then, obviously, we have a couple of meetings where we have to basically, come to certain conclusions, where we have to agree on certain things.” P1_Mng_Policy

The communication between the policy development team and relevant stakeholders during the review process takes a number of forms: meetings, workshops, interviews, emails, and a policy management system. For example, P2_Cons_Policy stated that:

“Normally what we do is set up a workshop. We invite key people from a particular section or the department in the organisation [relevant stakeholders].”

According to P1_Mng_Policy, P2_Cons_Policy, P3_Cons_Policy, and P5_Cons_Policy the review may occur in several iterations between the team and stakeholders to ensure changes suggested by stakeholders are considered in the final draft of the policy. P4_Mng_Policy stated that:

“It took another three to four months to develop ISP and because it actually went back and forth. We developed something, we sent it out to the different departments. They review their -- they came back to us and after several meetings and discussions and iterations, we were able to finalize it”

Practice 3-Activity 3: Approve the final policy draft
Once the policy document is finalised it should be signed and approved by the owner of that policy, who is usually an executive level manager.
After the review process is completed, the policy gets the approval, it is signed by the CEO.” P2_Cons_Policy

The importance of having clear ownership of the policy development process in enabling effective development and enforcement of the ISP was mentioned by two interviewees (P2_Cons_Policy and P3_Cons_Policy). P3_Cons_Policy reported a problem he faced in one of the organisation where they asked him to develop several policies. However, it was not clear who should approve the policy and sign it. P2_Cons_Policy suggested that there should be clear governing structure to avoid such situations.

6.4.2 The Implementation & Maintenance Stage

This section presents data related to management practices undertaken to implement the ISP. Three management practices were strongly supported by the five interviewees: (1) distribute the security policy, (2) communicate the security policy, and (3) enforce the security policy. Each practice consists of a number of activities.

Policy-Practice 4: Distribute the ISP

All five interviewees supported this practice and from the remaining twenty-nine, five interviewees mentioned this practice. The interviewees stressed the importance of making the policy available to employees. Two key activities were supported by the interviewees: (1) Select security policy delivery methods, and (2) Deliver the security policy.

Practice 4-Activity 1: Select security policy delivery methods

All five interviewees agreed that electronic delivery of the policy is the most common method for delivery in organisations. They reported different delivery methods such as email, policy portal, internal website and shared point.

“Organisations publish their policy on the intranet and this makes it available within the organisation”. P1_Mng_Policy

“Our organisation already has an information security policy developed which is available on the portal and which is electronically available to all the users.” P2_Cons_Policy.

Participants also stated that policy should be accessible for the stakeholders at all time. So they have the ability to refer to the document whenever they need.

Practice 4-Activity 2: Deliver the security policy

Once the delivery method is decided; the security policy documents are prepared in the right format usually electronically, then they will be uploaded on to the portal. Employees are notified
by email that the policy is available on the organisation’s webpage or on the portal and that they are required to read it and comply with it.

“whenever we have a new policy or an amendment is for our current policy we send a notification for key stakeholders to let them know that the final policy in the portal” P5_Cons_Policy

**Policy-Practice 5: Communicate the security policy**

All five interviewees pointed out that ensuring that their policies are read and understood by employees is a key gap in organisations. Fifteen interviewees in other ISMP areas also mentioned and highlighted its importance. Interviewees reported two common activities, that are undertaken by organisations to communicate the security policy to their employees. These activities are: (1) Ensure annual Training is conducted, and (2) Ensure the organisation provides ongoing awareness campaigns.

**Practice 5-Activity 1: Ensure annual Training is conducted**

Organisations conduct training programs for employees to ensure they are aware of the security policy and the repercussions of violating the policy. All five interviewees stated that the most common way to conduct the training program is computer-based training (CBT), where all employees will have access and go through the security policy.

“The best way [to communicate security policy] is to develop an internal portal [computer based training] CBT where the organisation can ensure that its employees have read and signed that policy.” P2_Cons_Policy

P1_Mng_Policy, P3_Cons_Policy, P5_Cons_Policy, and P4_Mng_Policy stated that another way of conducting training programs is by providing training sessions usually in the form of a presentation or briefing for employees, on the specific security policy that applies for that specific group of employees.

**Practice 5-Activity 2: Ensure the organisation provides ongoing awareness campaigns**

Another activity to communicate the security policy which has been pointed out by all interviewees is Ensure the organisation provides ongoing awareness campaign.

“There are multiple ways of doing it [communicating policy]. We were doing it through awareness campaign.” P3_Cons_Policy

According to the interviewees, an awareness campaign can take different forms such as poster, banners, etc. For more details on security awareness campaign see Chapter 7.
Policy-Practice 6: Enforce the security policy

The enforcement of the ISP was mentioned as a key policy management practice by all interviewees. Also, fifteen out of twenty-nine interviewees from other ISMP areas mentioned the enforcement of the security policy.

All five interviewees suggested three activities that can be undertaken to enforce policy in organisations: (1) implement technological mechanisms (2) conduct mandatory training program (3) implement penalties and disciplinary action.

Practice 6-Activity 1: Implement technological mechanisms

All Interviewees stated that they enforce policy by implementing technological controls.

“It’s [policy] enforced through different mechanisms depending on the nature of the policy. For example, some of the policies are predominantly around system level controls, so for policies and standards that related to identity and access management, the cryptography can be enforced through the implementation of technical measures.” P1_Mng_Policy

Further, examples of how policy can be enforced through different technological mechanisms are provided by P2_Cons_Policy, P4_Mng_Policy, P3_Cons_Policy, and P5_Cons_Policy. For instance, P4_Mng_Policy stated that in his organisation, there is a technological control that prevents employees from sending confidential documents using their email account.

Practice 6-Activity 2: Ensure mandatory training program is conducted

All interviewees also regarded that ensuring mandatory training program is conducted an as essential activity for enforcing the ISP:

“One of the ways to enforce policy is to provide mandatory training. This is regarded as one of the ways of enforcement” P5_Cons_Policy.

More discussion on the development of information security training is presented in Chapter 7.

Practice 6-Activity 3: Implement penalties and disciplinary action

An information security policy is also enforced through penalties and disciplinary action that are taken if the employees do not comply with the policy.

“the policy simply says if the policy is breached, then disciplinary action has to be taken. Disciplinary action means that an individual has to be penalised or he/she will be asked to leave the organisation, either of the two will happen. When I say penalise, probably here a warning will be given to him in form of a letter or document or whatever.” P2_Cons_Policy
According to P4_Mng_Policy and P5_Cons_Policy, the human resource (HR) department is to be notified whenever an employee has violated an ISP because HR has the ultimate responsibility for all employees in the organisation.

6.4.3 The Evaluation Stage

This section presents the findings and evidence on management practices relating to the review and evaluation of the ISP. Interviewees reported that organisations review their information security policy periodically. Following is a discussion of the review practice and activities that performed by organisations to review their ISP.

Policy-Practice 7: Review information security policy

There is consensus between the all participants upon the need to review the ISP in a periodic duration (i.e., usually six or twelve months). Interviewees discussed the importance of reviewing the security policy, how often it should be reviewed, and identified triggers for the review practice. Interviewees reported two key activities they undertake to review security policy: (1) Identify gaps in current policies and (2) Update policies and procedures.

Practice 7-Activity 1: Identify gaps in current policies

In this activity, there are a number of key documents that need to be examined to determine whether the organisation’s current policy needs to be updated. Through this activity the organisation should identify gaps in the management practices of the security policy (practices related the development and the implementation stages).

Relevant documents include regulatory and compliance requirements, business objectives, risk assessment reports and incident response report.

“In our organisation we review policy once a year. This year, we had to change it twice because there was a need, I think things which ACCC [Australian Competition and Consumer Commission] change.” P2_Cons_Policy

“If there is a major change in the environment in which you operate, or the system that you operate in that environment, whether procedural or technological, if there is a major change to either of those, you do a risk assessment and see what policies need to be updated.” P4_Mng_Policy

Examining incident reports can also trigger the creation of new policy or the review, communication and enforcement the existing ISPs that relate to a particular incident,

“The policies are often reviewed, but I think it's reviewed as we learn and investigate new incidents. And we apply what's happened in that incident to the
policy to make sure the policy is keeping up with what we're seeing in as far as security and the threat landscape. And do we need to add new policy or amend policy to cover those types of events?” P5_Cons_Policy

Interviewees also stressed the importance of relevant stakeholder feedback on evaluating the management practices of ISP. Therefore, interviewees indicated that one of the way to identify gaps in the current security policy is to collect feedback from participants about policy and the management practices. For example, P1_Mng_Policy, P4_Mng_Policy, and P2_Cons_Policy reported that they ask employees for feedback about the policy itself and the policy management practices.

“We constantly involve stakeholders in the process. For instance, we ask them to give us their feedback on things like how well the policy is communicated and enforced.” P5_Cons_Policy

P5_Cons_Policy argued that stakeholders’ feedback is a key factor that needs to be considered to improve the quality of ISP management practices.

**Practice 7-Activity 2: Update policies and procedures**

The participants reported that one of the main activities of the ‘review security policy’ practices is to update the policies and procedures. P4_Mng_Policy stated:

“the policy document is not static, it should be reviewed and updated regularly”

The participants also explained that based on the gaps which have been identified in the current policies, they update the policy to reflect the organisation’s security requirements.

Participants added that if a major change to the policies and procedures is required then they would follow the same process undertaken to develop the current document. Whereas if minor change is needed they would do the update in this stage.

6.4.4 Summary of the findings

This section discusses changes to the proposed framework of ISP management practices as a result of the empirical refinement and validation via semi-structured interviews with information security experts. The ISP area is a very mature compared to other areas of ISMP (risk management and incident response). The need for a methodological approach to developing, implementing and maintaining, and evaluating the ISP was recognised in a very early stage of the research in the domain. Therefore, several development lifecycles have been proposed in the literature.
However, the empirical data has provided rich understanding of the management process of ISP in organisations, which led to several changes to the preliminary framework. These changes include adding new activities to practices, renaming the practices, and changing the level from practice to activities. Table 6-5 presents the refined framework of information security policy management practices.

**Table 6-5 The refined framework of policy management practices**

<table>
<thead>
<tr>
<th>Stage</th>
<th>Practice</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Develop</strong></td>
<td>Establish policy development team</td>
<td>Determine the structure of the team</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Define roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>Determine organisation’s security needs</td>
<td>Identify security requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assess organisation’s current policies and procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify relevant stakeholders</td>
</tr>
<tr>
<td></td>
<td>Create security policy document</td>
<td>Develop initial security policy document</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop subsequent security policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Approve final policy draft</td>
</tr>
<tr>
<td><strong>Implement &amp; Maintain</strong></td>
<td>Distribute security policy</td>
<td>Select security policy delivery methods</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deliver the security policy</td>
</tr>
<tr>
<td></td>
<td>Communicate the security policy</td>
<td>Ensure annual Training is conducted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure the organisation provides ongoing awareness campaigns</td>
</tr>
<tr>
<td></td>
<td>Enforce the security policy</td>
<td>Implement technological mechanisms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure mandatory training program is conducted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Implement penalties and disciplinary action for noncompliance.</td>
</tr>
<tr>
<td><strong>Evaluate</strong></td>
<td>Review security policy</td>
<td>Identify gaps in current policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update policies and procedures</td>
</tr>
</tbody>
</table>

In the development stage, the participants reported that identification of relevant stakeholders actually happens during the gap and investigation of the organisation that undertaken as part of Determine organisation’s security needs practice. Therefore, identify relevant stakeholders activity was moved from the practice Establish policy development team.

In the Implementation & Maintenance Stage, the main practices of this stage did not change. However, activities within communicate the security policy practice and enforce the security policy were split into two and three activities respectively. This has been done as more understanding of the practices was gained through the descriptions of the participants.

The Evaluation stage has also not changed however, the participants provided rich information about how the review is conducted and triggers for the review practice of the ISP. The two
activities that were identified in the literature can be grouped to represent the activity *Identify gaps in current policy*.

### 6.5 Final validation

To perform the final validation of the framework an email was sent to each of the five focused interview participants to provide feedback on the framework and comments on whether the practices and key activities are comprehensive. All five participants have responded to the email with their comments and feedback on the framework.

For the first question “Do you think the framework covers key activities done in organisations to manage security policy?” Four of the participants answered that yes and they provided the following comments:

- “This framework could be used to provide the structure for detailed documents. The value to the end-user would potentially come from the detail.” *P1_Mng_Policy*
- “Yes, the framework looks good, it covers all the activities we do to manage security policy in my organisation” *P4_Mng_Policy*
- “Yes, the framework is okay” *P5_Cons_Policy*
- “I think from a consultant point of view; the framework reflects my experience of the process in different organisations” *P3_Cons_Policy*

While one participant (*P2_Cons_Policy*) answered ‘No’ and stated

> “I think that this is missing a key component of the process of understanding the business risks that the policy is attempting to address. A policy should only be created to solve a problem.” The participants suggested that “Identification and assessment of problem, eg risk assessment” should be added to the framework.”

Although the researcher agrees with the participants comments on the importance of understanding business risks, the researcher argues that the activity ‘Identify security requirements’ covers this point. In this activity, the result risk assessment process, which is undertaken as part of the risk management process, is used as an input to identify the organisation security requirements. Therefore, no change is done to the framework as a result of this comment.

The participant also comments on the review of the security policy. He stated

> “No mechanism is identified on how to inform this review process” *P2_Cons_Policy*

The activity *Identify gaps in current policies* includes reviewing relevant documents such as regulatory and compliance requirements, business objectives, risk assessment reports and
incident response report. Feedback is also collected and analysed to identify gaps in current policies. All these inputs are considered to be mechanism to inform the review process. Therefore, the framework of information security policy management practices has not changed as a result of the analysis of the final validation step.

6.6 Discussion

The analysis of the empirical data enabled a rich understanding to be gained of the managerial practices of ISP undertaken in organisations. The main contribution of this chapter is the identification of the set of key activities that are required to develop an ISP and the extent to which these activities are implemented in organisations. The set activities that have been identified is key to the policy management in organisations. No other activities were identified. The findings have provided an insight of how these activities have been institutionalised and how well they have been resourced.

6.6.1 Formal versus informal approach to the implementation of ISP management practices

The findings have provided evidence that can be used to identify the differences between the implementation of ISP management activities in organisations. Respondents from large organisations reported that they formally implement the set of activities to manage the ISP. Whilst in small organisations, because of a lack of resources (i.e., they do not have dedicated team for ISP) ISP management activities are dealt with more informally and occasionally may not be done at all. Following is discussion and insights from the empirical study.

The approach can be seen in various issues related to the implementation of policy management practices. These issues include the involvement of various stakeholders, undertaking a comprehensive investigation of the organisation’s context, and linking security objectives to business objectives. In light of the findings of this study, the remainder of this section compares and contrasts the formal and ad hoc approaches to the implementation of the ISP management practices.

Respondents reported that large organisations have a dedicated team for ISP management that consists of two or three personnel within the information security department, as well as a representative of relevant stakeholders. The findings suggest that in the formal approach, stakeholders have a more inclusive role in the implementation of ISP management practices.
On the other hand, respondents reported that small organisations do not have a dedicated team policy management rather the development is undertaken by staff from the IT department and/or delegated to an external security consultant. In addition, relevant stakeholders are not included in the process. This may be attributed to limited resources in terms of funds, expertise and support from top management for the implementation of the policy management practices.

The implementation of ‘Determine the security needs of the organisation’ practice differs in organisations. Respondents stated that some organisations conduct full gap analysis and investigation of the context using inputs such as risk assessment reports and incident response reports. The business goals and objectives are considered during the identification of the security objective to ensure they are well connected to the ISP. Other organisations might take informal approach by developing ISP without considering the context of the organisations and aim only to meet the regulatory and compliance requirements of developing an ISP which is not well communicated, enforced or periodically updated.

There are many differences between the formal and ad-hoc approach uncovered by the empirical data that have not been discussed throughout the literature. Although some of these findings are not surprising, they need to be discussed further and the underlying causes and repercussions of adopting the approach should be studied to improve the effectiveness of the ISP management process.

### 6.6.2 Stakeholders’ involvement in the process

Section 6.2.2, discussed the literature that emphasises the importance of involving stakeholders in the ISP management process. Several researchers (Flowerday & Tuyikeze, 2016; Maynard & Ruighaver, 2007; Safa et al., 2015) have highlighted the benefit of engaging stakeholders in the process, as it has a positive impact on both the quality of the policy developed and the acceptance of the policy by the stakeholders. This engagement will ultimately affect the communication and the enforcement of the policy, as stakeholders become aware of the policy in the early stage and are, therefore, more likely to comply and adhere to the policy. The findings from this study confirm that organisations are aware of the importance of involving stakeholders in the management of their ISP. The participants indicated that the ‘Identify relevant stakeholders’ activity and ‘Determine the composition of the policy development team’ activity, are undertaken as part of the ‘Determine the security needs of the organisation’ practice and ‘Establish information security policy development team’ practice respectively. By undertaking these practices organisations ensure that stakeholders are engaged in all stages of the policy
management process, and their feedback and inputs are considered during the investigation of the organisation’s context and security needs, the writing of the policy, the enforcement, and, lastly, the periodic review and update. A discussion of the study findings on the managerial practices undertaken to effectively communicate and liaise with relevant stakeholders during the process is presented in Chapter 9.

6.6.3 The role of external security consultants
The findings from this study show that many organisations delegate the development of their ISP to external subject-matter experts (information security consultants). While this approach may be a good indication that organisations are concerned about the quality of their ISP, there is a risk of developing a policy that is irrelevant to the context of the organisation, which could happen if the external security consultant is not given sufficient support and access to relevant documents and stakeholders to build a clear understanding of the context of the organisation. The consultant requires access to important documents to build a solid understanding of the organisation’s business goals and objectives and the security challenges faced by the organisation in the environment in which it operates. Thus, the sponsor who engages the security consultant should ensure full support for the process including access to documents and relevant stakeholders.

The security consultants should also constantly examine their understanding of the organisation, and refer to their sponsor whenever they confronted with issues that may prevent them from gaining a better understanding. To the best of our knowledge, this situation has not received attention in the literature relating to the provision of an ISP.

6.6.4 The implementation of a ISTA program to communicate and enforce policy
Traditionally, the enforcement of the policy is undertaken from a technological perspective, and little attention is given by organisations to the role that information security training and awareness can play in enforcing their ISP (Ifinedo, 2014; Kajtazi & Bulgurcu, 2013; Sommestad et al., 2014). This study findings indicate that organisations are focusing on the development and the implementation of ongoing security awareness programs and formal training sessions to communicate and enforce their ISP. This attention is aligned to the shift in the perception from seeing information security being mainly a technological problem to a more recognition of the importance of managerial practices(Soomro et al., 2016). Although more attention is
placed on using ongoing security awareness programs and formal training sessions, respondents indicated that communicating the policy is a key gap in many organisations. It is not known why this gap exists. However, this research speculates and questions the effectiveness of the awareness and training programs implemented in those organisations. Chapter 7 discusses the managerial practices undertaken to develop, implement and evaluate information security awareness and training (ISTA) program.

6.6.5 Inputs to the development process from other areas of ISMPs
Using the systems theory has enabled the researcher to identify the relationships between policy management and risk management, and incident response management. In accordance with the literature, the study findings show that risk management and incident response management provide inputs to policy management practices at two stages: the development stage and the evaluation stage. In the development stage, the policy development team reviews the organisation’s risk assessment reports and the incident response reports during the ‘Identify security requirements’ activity, which is undertaken as part of the ‘determine the security needs of the organisation’ practice. The findings of this study explain why several ISP development lifecycles (Al-Mayahi & Sa’ad, 2014; Rees et al., 2003) include conducting risk assessment as a part of the development process of the ISP. However, as the findings acknowledge the importance of having a recent risk assessment report during the development process, this thesis argues that undertaking a risk assessment process is part of the risk management process rather than the policy development process. Such a distinction is very important for understanding the interaction between ISMP areas as the practices of different areas of ISM may be undertaken by different team in the organisation. Being aware of this, the policy development team will have a better understanding of which team they should communicate for inputs to assist them in undertaking the managerial practices of the ISP. This distinction may have a positive impact on how the security program is managed in organisations where managerial practices from different areas of ISMP are well integrated and comprehensively implemented. Further results and discussion of the relationship between ISMP areas are presented in 10.3.2

6.6.6 Review and update the policy
The literature has emphasised the importance of reviewing the ISP periodically (Anderson Consulting, 2000; Lichtenstein & Swatman, 2001; Maynard, 2010; Palmer et al., 2001). Several authors have argued that the risk environment changes constantly, and if the policy is not
reviewed and updated to reflect the change in the risk environment, it is no longer meeting the organisation’s security needs (Maynard, 2010). This study confirmed the importance of the review process and provided insight on how the review is conducted in various organisations. The study shed light into how recent risk assessment and incident response report are used to assess the current policy and determine whether an update is required. This step is evident in the activity ‘Identify gaps in current policies’ undertaken by organisations as part of the ‘Review information security policy’ practice. Further, ‘update policies and procedures’ is an activity that is implemented to revise, updated, added or removed statements of the security policy document.

It is interesting to note that the review process in some organisations focused not only on the policy document, but also on the managerial practices undertaken as part of the policy management. The review practice includes assessing how well the policy is communicated and enforced in the organisations. For instance, when an incident occurs, the security manager will review the policy statement that addresses this particular issue as well as the practices and activities undertaken to communicate the policy, to determine whether proper procedures have been put in place to enforce the policy. This practice is extremely important, as it has not been outlined in the literature relating to the review of ISP.

6.6.7 External factors such as compliance and audit and their influence on the development process

The intent of the organisation from the development of ISP plays a significant role in the implementation of the managerial practices. Organisations that understand the value of information security for achieving the business objectives and gaining competitive advantage tend to pay attention to the implementation of managerial practices of the ISP as it ensures a formal process is followed to develop an effective ISP that is applicable to the context of the organisation.

On the other hand, organisations, that develop policy to meet the regulatory and compliance requirements do not implement policy management practices in a formal way. In other words, the developed ISP are usually copy and paste from security management standards and other organisations’ policies. Consistent with the literature, the findings indicate that this approach may have a significant impact on the developed ISP, as it may be irrelevant to the context of the organisation and not connected to its business objective, which ultimately affect the
enforcement of the policy and the effectiveness of the information security management process.

The external and internal audit process also has an impact on the implementation of ISP managerial practices. The data shows that audit can trigger the review and update of security policy.

6.7 Summary
This chapter presented the development and refinement of ISP management practices framework. An overview of the literature on ISP was provided, highlighting gaps and deficiencies related to the provision of an ISP. Then a framework was developed based on a rigorous and systematic review of the literature. The refinement and validation of the proposed framework is also presented. The chapter ended discussion of the findings from the empirical data obtained from the interviews and outline of the contribution. The next chapter will present the second area of ISMP, which is information security training and awareness (ISTA). This includes review of the literature, framework development, empirical findings and analysis to refine the framework and discussion related to this area.
Chapter 7 INFORMATION SECURITY TRAINING AND AWARENESS MANAGEMENT PRACTICES

7.1 Introduction
The previous chapter presented the development and validation of a security policy management practices framework. This chapter discusses the results of the comprehensive review and analysis of the literature relating to information security training and awareness (ISTA). The aim of this chapter to develop a comprehensive ISTA framework based on the literature and then validate the ISTA framework.

This chapter is organised as follows. Section 7.2 provides background information on the ISTA program and its importance, and an overview of the current state of the research on the area. Section 7.3 presents the proposed framework of ISTA management practices. Section 7.4 presents empirical data from expert interviews that were conducted to refine the proposed framework. Section 7.5 presents the analysis and findings from the follow up interviews which were conducted for final validation of the framework. Section 7.6, discusses the contributions and implications of the proposed framework of ISTA management practices, and Section 7.7, provides a summary of the chapter and introduces the next chapter.

7.2 Literature review
Information security training and awareness (ISTA) program refer to organised information security training activities that are related to security training, and awareness raising programs (Crossler and Bélanger 2006; D’Arcy et al.2009). The main aim of the ISTA program is to change the behaviour of employees towards security and encourage good security practices (De Maeyer, 2007; Frye, 2007). Several researchers stated that there are three different levels of learning activities in regard to information security: building in-depth knowledge that is
required to design and implement a security program (Education), develop skills and knowledge to enable employees to perform their job in a secure manner (Training), and raise the awareness of the employees about risk and security (Awareness) (Mani, Mubarak, & Choo, 2014; Whitman, 2008; Whitman & Mattord, 2012). These three elements: education, training and awareness constitute the ISTA program.

Security Education is mainly for security professionals such as information security officer, security manager and security consultant. Security education aims to create information security professionals by providing in-depth knowledge about various functions of security and multi-disciplinary perspectives of security issues (technological, managerial, and social).

Security training aims to provide employees with an adequate level of skills to enable them to perform their job securely. Several authors (e.g., Puhakainen & Siponen, 2010; Siponen et al., 2014; Sommestad et al., 2014) recommend security training for general users to increase their compliance with the ISP by involving users actively in issues addressed by the ISP such as password management, good security practice and reporting security incidents (Whitman & Mattord, 2008). Security training can be provided for technical users as required according to their responsibilities.

Security awareness involves providing general employees with information and informal training about security to assist them to understand the importance of information security and act accordingly (Whitman & Mattord, 2008). Table 7-1 depicts a comparison between the ISTA program’s elements.

Although these three elements (education, training and awareness) provide three learning levels and target three different groups within the organisation, the use of terminology to describe activities related to these elements in the literature is not consistent with their definitions and purpose. Several terms are used in the literature such as ‘security education, training and awareness (SETA)’, ‘security training’, ‘information security awareness’, and ‘security awareness training’. (Tsouhou, Kokolakis, Karyda, & Kiountouzis, 2008) reviewed existing literature on the distinction between security awareness, training and education. They concluded that while researchers (e.g., ENISA, 2010b; Kritzinger & Smith, 2008; Vroom & Solms, 2002) make a clear distinction between security awareness, training and education, the majority of
researchers did not differentiate between these three elements and use them interchangeably in a conflicting and ambiguous manner.

Table 7-1 A comparison between ISTA program’s elements adopted from Whitman and Mattord (2008).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Awareness</th>
<th>Training</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
<td>Information</td>
<td>Knowledge</td>
<td>Insight</td>
</tr>
<tr>
<td>Objective</td>
<td>Recognition and retention</td>
<td>Skill</td>
<td>Understanding</td>
</tr>
<tr>
<td>Teaching method</td>
<td>Media</td>
<td>Practical Instruction</td>
<td>Theoretical Instruction</td>
</tr>
<tr>
<td></td>
<td>- Videos</td>
<td>- Lecture</td>
<td>- Discussion seminar</td>
</tr>
<tr>
<td></td>
<td>- Newsletters</td>
<td>- Case study workshop</td>
<td>- Reading and study</td>
</tr>
<tr>
<td></td>
<td>- Posters</td>
<td>- Hands-on practice</td>
<td>- Research</td>
</tr>
<tr>
<td>Impact Timeframe</td>
<td>Short-term</td>
<td>Intermediate</td>
<td>Long-term</td>
</tr>
</tbody>
</table>

Practices and activities undertaken in organisations usually fall under the training and awareness definitions, while education is typically done in specialised security education institutes and universities (Whitman & Mattord, 2008; Wilson & Hash, 2003). Therefore, the term information security training and awareness (ISTA) is used throughout this thesis.

7.2.1 The importance of ISTA

In Chapter 5 which addresses information security policy (ISP) management practice, the ISTA program was identified as an essential element for communicating and enforcing the ISP. Several researchers (Bacik, 2008; Hare, 2002; Lowery, 2002; Patrick, 2002) consider the development of the ISTA program to be part of the ISP development lifecycle while others (Hu et al., 2012; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2010; Tsohou et al., 2008) argue that an ISP is a prerequisite for the development of an ISTA program. Either way, ISTA and policy are inherently connected as part of the organisation’s information security strategies.

There is a wide consensus in the literature on the need for an ISTA program to protect organisational information assets (Khan, Alghathbar, & Khan, 2011; Mani et al., 2014; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Vroom & Solms, 2002). In fact, existing information security management frameworks (Chaudhry et al., 2012; Kritzinger & Smith, 2008; Zuccato, 2007) integrate the ISTA program with other information security functions.
such as security policy, risk management and incident management. For example, ISO 27001 Information technology - Code of practice for information security management stresses the need for an ISTA program as part of an overall management system of information security within the organisation. The standard recommends that organisations should provide “an adequate level of education, training and awareness in security procedures and correct use of information systems for all employees” (p.25).

Recent security reports show that security incidents are continually increasing, and that insiders cause a significant proportion of reported incidents (2014 Internet Security Threat Report; ENISA Threat Landscape 2013). This situation indicates that having ISP and technological controls in place are not enough to mitigate risks. Many studies (e.g., D’Arcy et al. 2009; ENISA 2010; Hu et al. 2012; Kim 2014; Abdul Molok, Ahmad, & Chang, 2010) suggest that an ISTA program should be in place to make employees aware of security risk, and provide them with the required skills and knowledge to comply with the ISP. Moreover, an ISTA program will ensure that employees perform their job in a secure manner.

7.2.2 Focus of the literature on ISTA
The recognition of the importance of the ISTA program for protecting the organisation from various types of risks related to the human factor has led to considerable research in the area. One major focus of the ISTA literature is on providing practical guidance for the development, implementation and evaluation of the ISTA program (ENISA, 2010b; Herold, 2010; PCI, 2014; Roper, Grau, & Fischer, 2006; Wilson et al., 1998). Another focus is on studying the impact of implementing an ISTA program on user compliance with security policy (Li et al., 2014; Safa et al., 2015; Siponen et al., 2014), top management support (Puhakainen & Siponen, 2010), and establishing security culture (Alnatheer, Chan, & Nelson, 2012; Da Veiga & Eloff, 2010; Karlsson & Hedström, 2014; Ruighaver et al., 2007).

7.2.3 ISTA program development
The importance of an ISTA program for safeguarding information assets has led many authors to recommend the establishment of an ISTA program within organisations as part of their security program (Öğütçü et al., 2016; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). There are a number of publications (Croasdell, Elste, & Hill, 2018; De Maeyer, 2007; Hansche, 2001; Khan et al., 2011; Peltier, 2005; Valentine, 2006; Vincent & Ross, 2001; Vroom & Solms, 2002; Whitman, 2008) NIST, ENISA that provide guidelines for organisations on how to develop an
ISTA program. Approaches and models proposed in these studies and guidelines consists of different stages each stage have several activities, that it can be summarised in three types of activities: (1) development, (2) implementation and (3) evaluation of the ISTA program. Following is a discussion of the existing approaches and models for developing ISTA programs.

1) Development Phase Activities

The development phase includes activities used to: understand the current situation of the organisation, obtain management support and acquire needed resources to develop an effective program (Bowen et al. 2006; Power and Forte 2006). These activities include conducting a needs assessment for an ISTA program, defining goals and objectives, establishing the ISTA development, and identifying the target audience for ISTA program. The literature discusses the importance of understanding the needs of an organisation and designing an ISTA program that meets these specific needs. For instance, Peltier (2005) contends that an effective ISTA program should consider the needs and current level of training and awareness, and have a sufficient understanding of the target audience of the program. In the same vein, Valentine (2006) proposes an ISTA program approach that begins with an Assessment phase followed by Identification and Education phases. In terms of setting goals and objectives, many researchers stress the importance of defining achievable and measurable goals and objectives for the ISTA program (Peltier 2000). Development phase activities also include developing the materials for ISTA consisting of tasks around topic selection according to the identified needs (ENISA 2010; Johnston and Warkentin 2010).

2) Implementation Phase Activities

The Implementation phase focuses on the conduct of the ISTA program using a variety of delivery methods. The literature on the implementation of the ISTA discusses methods of effectively delivering ISTA messages. Several authors recommend the use of a combination of methods for delivery, such as newsletters, email, awareness tools (e.g., pen and notepads) and posters to convey the security message to the intended audience (Abawajy 2014; Peltier 2005).

3) Evaluation Phase Activities

The final phase within the ISTA program development process is evaluation where the organisation reviews and evaluates their ISTA initiatives to measure their effectiveness. Effectiveness is usually measured through identifying changes to employees’ behaviour towards information security (Öğütçü et al. 2016). Existing approaches for managing an ISTA program,
focus on evaluating the knowledge obtained for the program (PCI 2014). This is a very limited view of evaluation. Evaluation should also focus on the effect of ISTA on the overall security of the organisation because of the change in employees’ behaviour (Tsohou et al. 2015). One manner to measure the effect of ISTA is to compare the number of security incidents as a result of noncompliance with security policy prior to and after the ISTA programs implementation (Thomas, George, & Yaojie, 2018).

7.2.4 ISTA approaches
Kajzer, D’Arcy, Crowell, Striegel, and Van Bruggen (2014) conducted a survey of 293 users to explore the relationship between awareness message themes and individuals. The result of the study suggests that the effectiveness of awareness messages vary depending on personality. The result may aid the ISTA development team to increase the effectiveness of the program by selecting an appropriate message for an employees’ personal profile. The finding of Kajzer et al. (2014) supports Vincent and Ross (2001)’s argument that to provide effective training, individual learning style and personality type should be considered when developing a training program.

De Maeyer (2007) conducted field research that involved a discussion with peer security officers and consultants. Based on feedback from the participants, the author identified two deficiencies in the existing ISTA program that made the program ineffective: the lack of preparation of the program and inaccurate evaluation. The lack of preparation includes not having clear objectives, lack of support from top management, not address the needs for target group within the organisation, and not using specific material to address the needs. In regard to the inaccurate evaluation of the program is focusing the assessment of the program on the security knowledge rather than on the behaviour. De Maeyer (2007) also argued that the information security team and relevant stakeholders should be involved in the development process of the ISTA program to increase their understanding of the importance of security and, therefore, create a culture of security.

Vroom and Solms (2002) developed a model for the development of information security awareness. The authors provided a practical implementation of the proposed model through a suggestion to implement the program using awareness website. The website should have different sections namely, introduction logon, security policies, questionnaire, tutorial, and knowledge base.
Another practical approach for information security awareness and training was developed by Power and Forte (2006). The authors conducted a case study on a global entity to propose a three phases information security awareness and training program. In Phase I, the aim is to engage all employees economically and effectively in the security process of the organisation. It entails five activities: 1) create a project team that consists of participants from IT, Human Resources, Risk and other relevant stakeholders, 2) lunch a bi-monthly newsletter about security issues, 3) include a 45-minute presentation about security responsibilities in the orientation of new employees, 4) establish an annual observed security day, 5) Develop a 45-minute eLearning program for employees. Phase II: includes conducting two-day technical security seminars for IT professionals and doing further improvement on activities undertaken in the previous phase. Phase III delivers vital intelligence and early warning to the executives, and involves briefing top executives of the organisation about security (incidents report and risk assessment) and measuring the effectiveness of the ISTA program.

Power and Forte (2006) further conducted a survey of IT directors and managers within the organisation to evaluate the proposed program. The results indicated that the global security team established in Phase I had strengthened the security of the organisation. The survey reported that participants of the global training day thought the training seminars were effective.

Puhakainen and Siponen (2010) asserted that there is a lack of training approaches that are based on theory and empirically evaluated. Therefore, they proposed a training program based on the universal constructive instructional theory and the elaboration likelihood model. Puhakainen and Siponen (2010) evaluated the training program through an action research project. The study offers valuable recommendations, including the use of messages and delivery methods that activate and motivate employees.

Another example of an ISTA model based on theory was presented by Khan et al. (2011). The authors argued that current methods for awareness campaigns focus on providing information and knowledge of security practices and neglecting the motivation and behavioural skills aspects. Khan et al. (2011) proposed a model to develop an effective security awareness campaign. The model is based on healthcare, Information-Motivation-Behaviour skills (IMB) and environmental awareness (Normative Social Norms). The model suggests that an awareness campaign starts with developing normative social norms through social interaction. Normative social norms will have a positive impact on personal and social motivation, and motivation will
have a positive influence on changing employees’ behaviour, which will eventually increase information security awareness.

Karjalainen and Siponen (2011) surveyed the existing ISTA development approaches, and categorised them into seven categories based on their approach, then developed a metatheory that proposes four pedagogical requirements that should be satisfied by any security training approach. Theoretically grounded recommendations were provided for the design of the programmes.

Puhakainen and Siponen (2010) stressed the need to design a systematic ISTA program. This chapter aims to develop a comprehensive framework for ISTA program management practices. The proposed framework provides guidance for organisations on how to manage their ISTA program. The focus of the propose framework is to provide sufficient and coherent guidance for organisations to manage their ISTA program effectively. Learning and behaviour theories, materials design and presentation skills are not the focus of this research.

### 7.2.5 The Effect of ISTA on policy compliance

In the early stages of ISTA research researchers mainly focused on providing the knowledge and skills to make employees aware of the security problem. However, several researchers argue that making the user aware of a security issue is not enough; rather, the ISTA program should go beyond basic awareness towards influencing employees’ behaviour and creating a culture of security (Abdul Molok, Ahmad, & Chang, 2011c; D’Arcy, Hovav, & Galletta, 2009; Hu et al., 2012; Ruighaver et al., 2007; Warkentin, Johnston, & Shropshire, 2011).

Several studies in policy compliance and employee behaviour have concluded that an ISTA program has a significant effect on employees’ adherence to their organisation’s security policy (Abdul Molok, Ahmad, & Chang, 2011b; Albrechtsen & Hovden, 2010; Furnell & Rajendran, 2012; Vroom & von Solms, 2004). These studies have used different theories to understand employees’ behaviour, actions, attitudes, and perceptions towards information security and what make them comply and adhere to an ISP. Several recommendations were provided to organisations on how to develop an effective ISTA program.

### 7.3 The proposed ISTA management practices framework

As described in Section 4.3.2, a comprehensive and rigorous review of the ISTA literature was conducted. The following search terms ‘security awareness and training’, ‘security awareness
program’, ‘information security awareness training’ and security education, training and awareness’ were used to search in various databases and search engines. See Section 4.3.2 for more details on the search and analysis process of literature related to ISMP areas.

The overall understanding that emerged from the comprehensive review and coding process resulted in the development of a framework of ISTA management practices. This section discusses the proposed framework. Table 7-2 depicts the framework which consists of three main stages: the Development stage, the Implementation & Maintenance stage, and the Evaluation stage. Each stage consists of a number practices, each having a number of key activities.

### 7.3.1 The Development Stage

The development stage consists of all the practices associated with development of ISTA program in an organisation. There are four practices within the development stage.: (1) conduct needs assessment for ISTA program, (2) establish ISTA development team, (3) develop a plan for the ISTA program, and (4) develop ISTA materials. Each practice has one or more key activities.

**ISTA-Practice 1: Conduct needs assessment**

The first practice in the development stage is to conduct a needs assessment for ISTA program. Conducting a needs assessment aims to determine the organisation’s ISTA needs (Vincent &
Ross, 2001; Whitman, 2008; Wilson & Hash, 2003). Peltier (2005) stated that understanding stakeholders’ needs is the first step in establishing an effective information security program. This can be applied to ISTA program as well.

This practice involves two activities: (1) identify the needs for the ISTA program through examining security policy, incident response report and job’s roles and responsibilities, and (2) review existing ISTA activities in the organisation and

**Practice 1-Activity 1: Identify the needs for ISTA**

According to Herold (2010), the needs for ISTA can be identified through (1) information security policy, (2) incident response report and (3) job’s roles and responsibilities. This will help the organisation to identify the current level of training and understanding of the employees.

The information security policy should be used as an input to determine employees’ needs for ISTA (D’Arcy et al., 2009). Tsohou et al. (2010) considered the ISTA program to be a prerequisite for successful implementation of the ISP in the organisation. To ensure that employees adhere to the organisation’s ISP, employees need to have appropriate skills and awareness of the policy (D’Arcy et al., 2009; Parsons et al., 2014). For example, if an ISP of an organisation asks employees to use antivirus software and update it regularly, employees need to be aware of the types of antivirus software that are available, how to install it, and how to update it.

Another source for identifying the needs for ISTA is the security incidents report. The security incident response report provides information on what security issues employees need to be aware of, and what skills employees need to have to prevent an incident from happening (ENISA, 2010b). For example, if an incident response report indicated that unauthorised access has taken place due to a weak password, then employees should be trained on how to set strong passwords, and their awareness needs to be raised of risks associated with weak passwords.

The roles and responsibilities of information security personnel can also be used to identify the organisation’s needs for ISTA (Wright, 2005). Information security personnel such as the chief information security officer, security manager, security administrator and analyst, and security technician, have specific roles and responsibilities. Individuals who hold these positions need security training and education to undertake the roles and responsibilities required by these positions to maintain the organisation’s security requirements.
Furthermore, each ISMP area (security policy, risk management, incident response) that has been identified in this research has a number of practices. These practices require specific skills and knowledge for protecting organisations from risks. For instance, incident response team members should have the right skills to respond to a security incident to prevent any damage to the organisation (Ahmad, Hadgkiss, et al., 2012; Smith, 1994).

**Practice 1-Activity 2: Review existing ISTA program**

If there is an existing ISTA program, the organisation should collect data about the existing ISTA program (Peltier, 2005; Wilson & Hash, 2003). Information obtained from the review process of the existing ISTA program is useful to determine the skills and knowledge that existing ISTA address and identify ISTA materials and methods used to deliver these materials. If a formal evaluation has been conducted of the existing ISTA program, the output from the evaluation can be used to identify gaps and possible ways for improvement.

**ISTA-Practice 2: Establish ISTA development team**

The second practice in the development stage is to establish an ISTA development team (ENISA, 2010b; Manifavas, Fysarakis, Rantos, & Hatzivasilis, 2014; PCI, 2014; Tsohou et al., 2010). This team is responsible for undertaking development, implementation and evaluation activities for managing the ISTA program in organisations. The organisation should ensure that employees with the required skills should be engaged in the planning for the ISTA program. The team should be assembled from different departments within the organisation (ENISA, 2010b; PCI, 2014). For example, the team should involve experts in information security, organisational culture, curriculum development, social marketing, and behaviour change (Maqousi, Balikhina, & Mackay, 2013; PCI, 2014; SANS, 2016). The size of the team will depend on the specific needs of each organisation and its culture (PCI, 2014).

**Practice 2-Activity 1: Identify roles and responsibilities**

Roles and responsibilities for managing the ISTA program in organisations include assessing the needs, developing the plan, developing the materials, conducting and evaluating the program (ENISA, 2010b; Hansche, 2001; Wilson & Hash, 2003). People who should be involved in managing the ISTA program include: managers, security specialist, and training professionals.
Table 7-3 provides a summary of the ISTA program’s key roles and their responsibilities.

Table 7-3 summary of the ISTA program’s key roles and their responsibilities (Wilson, de Zafra, Pitcher, Tressler, & Ippolito, 1998).

<table>
<thead>
<tr>
<th>Roles</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Management All levels including team leaders, program managers, system managers, and organisation leaders | To determine staff training needs  
To evaluate training effectiveness  
To prioritize use of training resources |
| IT Security Specialists              | To gain an understanding of IT security requirements and the knowledges, skills, and abilities needed to meet those requirements |
| Training Professionals (Career Planners/Human Resource Personnel, Training Coordinators, Curriculum Developers, Course Developers, Trainers) | To evaluate course quality  
To assist in obtaining appropriate courses and materials  
To develop or customize courses/ materials |

In addition, a representative from the ISTA program’s target groups to provide inputs on the needs assessment and feedback of initial materials and the overall effectiveness of the ISTA program (ENISA, 2010b; Wilson & Hash, 2003).

**ISTA-Practice 3: Develop a plan for ISTA program**

An effective ISTA program requires extensive planning activities. Planning for the ISTA program is a vital practice in managing the program, as it provides justification for the ISTA program and the required resources to conduct it (Herold, 2010; Nosworthy, 2000; Wilson & Hash, 2003). Developing an ISTA plan consists of several activities: (1) define goals and objectives, (2) establish development team for ISTA, (3) identify roles and responsibilities, and (4) identify target group for ISTA.

**Practice 3-Activity 1: Define goals and objectives**

The first activity of the ISTA plan is to define the goals and objectives of the ISTA program. The organisation needs to state the overall objectives of the ISTA program (ENISA, 2010b; Wilson & Hash, 2003; Wright, 2005). Goals and objectives of the program should be short, achievable, and measurable. Hansche (2001) contends that when identifying the goals for the ISTA program, the overall mission and goals of the organisation should be taken into
consideration. Clear objectives are important for effective management of the ISTA program (ENISA, 2010b).

The overall goal of an ISTA program is to improve the information security of the organisation (Abawajy, 2014; Lebek, Uffen, Breitner, Neumann, & Hohler, 2013; Siponen, 2001). This goal can be achieved by raising employees’ awareness and understanding about the information security issues and as a result, improving their behaviour towards information security. Improving information security in the organisation can be also achieved by training the employees to acquire the appropriate security skills to enable them to perform their job in a secure manner (Whitman, 2008).

Whitman and Mattord (2008) explain that the ISTA program has three main objectives: building in-depth knowledge to develop, implement, and evaluate the information security program for an organisation, developing skills and knowledge of employees to enable them to perform their job securely, and improving awareness of the need to protect the organisational information assets.

**Practice 3-Activity 2: Establish a schedule ISTA program**

Several authors stated that establishing a schedule for the ISTA program is one of the main elements of the ISTA plan. Wilson and Hash (2003) states that once the ISTA program’s goals and objectives have been finalized, an implementation schedule must be established. The schedule should include a list of ISTA program’s activities (e.g., annual training, awareness newsletters or email) and when it will be implemented (Herold, 2010; Wilson et al., 1998; Wilson & Hash, 2003). The activities should be prioritised according several factors including availability of materials and resources, roles and organisational impact, and compliance and regulatory requirements (Herold, 2010; Khaled, Peggy, & Michael, 2018; Thomas et al., 2018).

**Practice 3-Activity 3: Identify Target group for ISTA program**

The result of the needs assessment for the ISTA program will give an indication of the target groups of each element for the ISTA program (ENISA, 2010b; Vroom & Solms, 2002). For example, if an ISP is being implemented, employees who will be affected by the policy are the targets for the awareness program. The implementation of security tools will require the organisation to train employees who are responsible for using these tools. Training will provide employees with the necessary skills and knowledge to perform their job in a secure manner (Gaunt, 1998).
Target groups or audiences of the ISTA program can be segmented according to their job responsibilities, which will enable the ISTA development team to identify the ISTA needs for this particular group by examining their roles. For instance, information security personnel will require training to implement technological controls as an important element of the information security program. However, general staff in the organisation only need an awareness campaign to raise their awareness about the ISP and procedures of the organisation. Table 7-4 shows an example of groups that can be the targeted for ISTA program. (ENISA, 2010b)

Table 7-4 Example of groups that can be targeted for ISTA program (ENISA, 2010b)

<table>
<thead>
<tr>
<th>No</th>
<th>Target Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Employee</td>
<td>All organisations’ personnel.</td>
</tr>
<tr>
<td>2</td>
<td>Mid-level manager</td>
<td>Managers throughout the organisation responsible for personnel activities and performance. Often not technically oriented, this group needs to be educated and understand the importance of information security. This will allow them to implement the relevant security policies and controls within their business areas.</td>
</tr>
<tr>
<td>3</td>
<td>Executive management</td>
<td>Executive managers are the key decision-makers for investment in security.</td>
</tr>
<tr>
<td>4</td>
<td>System administration</td>
<td>Technically inclined personnel, usually responsible for the settings and security of network servers and security systems.</td>
</tr>
<tr>
<td>5</td>
<td>Third party</td>
<td>Partners, suppliers, consultants contracted to perform a work in an organisation. Gartner reported that a troubling new California data security breach demonstrates the urgent need for enterprises to require more rigorous security practices from outside contractors</td>
</tr>
</tbody>
</table>

ISTA-Practice 3: Develop ISTA materials

Developing ISTA materials is an important practice (ENISA, 2010b; Hansche, 2001; Maqousi et al., 2013). It comes after defining the goals and objectives of the program and identifying the target groups, as knowing the target audience and their needs are key issues, that must be considered while designing ISTA materials (Hansche, 2001; Herold, 2010). According to Maqousi et al. (2013) In this practice, the critical topics that have been identified through the needs assessment will be used to develop ISTA material and select the optimal means to deliver them. Therefore, this practice involves three key activities (1) determine the ISTA message, (2) Select ISTA program delivery techniques, and (3) construct the materials.
Practice 3-Activity 1: Determine the ISTA message

There are two types of messages that should be determined: training messages and awareness messages. Each type of message should fulfil its aims and objectives that has been identified in the planning activities for the ISTA program. The aim of security training material is to provide employees with the necessary skills and knowledge to perform their job securely (Arthur Jr, Bennett Jr, Edens, & Bell, 2003). The goal of awareness materials is to encourage employees to comply with the ISP (Abawajy, 2014).

In terms of the security training messages, the result of the needs assessment will assist the organisation to answer the question of what skills they want the target group (employees) to learn and apply? (Whitman & Mattord, 2008). They divided training inside the organisation into three categories: (1) training for general users, (2) training for managerial users, and (3) training for technical users. Training for general users aims to ensure that users have read and understood the policy. It provides an opportunity for users to ask questions and receive guidance on how to comply with the ISP. Training for general users will also provide general users with technical skills such as password management and incident reporting. Training for managerial users should include general users’ training skills and also skills to manage the organisation’s security program. The third category of training is training for technical users. It aims to provide technical skills for IT staff and security staff.

The awareness message should be short, direct and simple. There are two questions that should be asked before selecting awareness topics: what behaviour does the organisation wants to reinforce? and, what issues does the organisation want the employees to be aware of? Wilson and Hash (2003) give examples of awareness topics:

- Password usage and management, including creation, frequency of changes, and protection.
- Protection from viruses, worms, Trojan horses, and other malicious code
- The ISPs – implications of noncompliance.

Practice 3-Activity 2: Select ISTA program delivery techniques

Organisations can utilise different delivery methods to teach their employees the necessary skills (Abawajy, 2014). The target audience, and the skills organisations want their employees to acquire, play an important role in the process of selection of delivery methods for the ISTA program (Abawajy, 2014; Tsohou et al., 2008). Table 7-5 shows a summary of the most common delivery methods adopted from (Whitman & Mattord, 2008).
The awareness message can be delivered using various methods, such as messages on awareness tools posters, “do’s and don’t lists,” or checklists, newsletters, organisation’s wide email message, videotapes, etc (Abawajy, 2014; Hansche, 2001).

### Practice 3-Activity 3: construct the materials

In this activity, the ISTA development team construct and design the materials and prepare it to be published and distributed as part of the implementation and maintenance stage. The literature reports two common approach regarding the development of ISTA materials (ENISA, 2010b; Herold, 2010; PCI, 2014). The first approach is to develop new materials to address the organisation’s needs for ISTA. This could be done by either the ISTA program development team or outsourced to specialised ISTA agencies. The second approach is to acquire existing materials from different sources. There are a variety of sources of ISTA material that can be incorporated into an ISTA program. However, a thorough review of existing material should be conducted to determine whether these materials would be useful and suit the needs of the program (ENISA, 2010b). Existing materials can describe how to begin to develop an entire awareness program, session, or campaign (Wilson & Hash, 2003).

ISTA material can be developed using one theme at a time or created by combining a number of themes or messages into a presentation. For example, a poster or a slogan on an awareness tool should contain one theme, while an instructor-led session or web-based presentation can

---

### Table 7-5 Summary of the most common delivery methods adopted from (Whitman & Mattord, 2008)

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-on-One</td>
<td>A dedicated trainer works with each trainee on the area specified.</td>
</tr>
<tr>
<td>Formal Class</td>
<td>A single trainer works with multiple trainees in a formal setting.</td>
</tr>
<tr>
<td>Computer-Based Training</td>
<td>Pre-packaged software that provides training at the trainees’ workstation.</td>
</tr>
<tr>
<td>Web Seminars</td>
<td>Trainees receive a seminar presentation at their computer. Some models allow teleconferencing for voice feedback; others have text questions and feedback.</td>
</tr>
<tr>
<td>User Support Group</td>
<td>Support from a community of users is commonly facilitated by a particular vendor as a mechanism to augment the support for product or software.</td>
</tr>
<tr>
<td>On-the-Job Training</td>
<td>Trainees learn the specifics of their jobs while working, using the software, hardware, and procedures they will continue to use.</td>
</tr>
</tbody>
</table>

---

The awareness message can be delivered using various methods, such as messages on awareness tools posters, “do’s and don’t lists,” or checklists, newsletters, organisation’s wide email message, videotapes, etc (Abawajy, 2014; Hansche, 2001).
contain numerous themes. Regardless of the approach taken, the amount of information should not overwhelm the audience.

Once the first draft of the material is created it should be shared with representative stakeholders and primary contacts to obtain feedback. Several guidelines stressed the importance of involving stakeholders not just in reviewing the material but the entire management process of the ISTA program. (Herold, 2010) stated that “Build the learners’ interest and demand by involving them early in the development lifecycle and sustain their involvement throughout the life of the training. This way you also help to ensure the content will be something your learners will relate to and be engaged in learning about” (p.182).

The review of the material should focus on accuracy, technical soundness, and instructional appropriateness for the target group. Feedback should be incorporated and a final check is conducted with the team and at least one representative of the target group (Herold, 2010). Once the material is finalised it’ll be ready to be used in the implementation stage.

7.3.2 The Implementation and Maintenance Stage
The implementation and maintenance stage represents all the practices associated with communicating the program, explaining its importance to the employees, and implementing the ISTA program. This stage consists of one practice: conduct ISTA program.

ISTA-Practice 5: Conduct ISTA program
Conducting the ISTA program is where the actual implementation of the ISTA program is carried out. It involves two main practices: (1) conduct training session and (2) start the awareness campaign.

Practice 5-Activity 1: Conduct training session
The training program is conducted using the developed materials and selected delivery methods. One of the most common and popular training delivery technique is given presentation by instructor onsite. Effective presentation’s skills and teaching methods should be used (Ahmad & Maynard, 2014; Bowen et al., 2006).

Technologies should be utilised to deliver training. Examples of delivery techniques that are reported in the literature include interactive video training and computer-based training. Many researchers suggest that blending various training delivery techniques in one session can be an effective way to present material and hold an audience’s attention. For example, showing videos
during an instructor-led session allows the audience to focus on a different source of information.

**Practice 5-Activity 2: Start the security awareness campaign**

The awareness campaign starts by using the materials developed and the selected delivery methods (Wright, 2005). It may include sending awareness materials through emails or putting posters in noticeable places inside the organisation, such as common rooms, lifts, etc.

The literature suggests that organisations should present the awareness material using a variety of ways making the interesting and current, repeating an awareness message to increase users’ attention of awareness lessons or issues (Herold, 2010).

Unlike training which is more formal and structure, awareness activities are less formal, occur in an ongoing basis, use a wide range of delivery methods, take less time and should catch the attention of the target audience by being more creative and fun (Herold, 2010).

It is critical to remember that an awareness program never ends. An effective awareness program must repeat the message multiple times in many ways. The more important the message, the more often it should be repeated using multiple methods. Because it is an ongoing activity, it requires creativity and enthusiasm to maintain the interest of all audience members (Herold, 2010; Nosworthy, 2000; Vincent & Ross, 2001).

### 7.3.3 The Evaluation Stage

The evaluation process will serve as an input for the development stage of the ISTA program. It will provide detailed feedback to enable the organisation to change its ISTA program plan, and update materials and delivery methods. The evaluation stage involves one key practice, which is to review the ISTA program periodically.

**ISTA-Practice 6: Review ISTA program periodically**

Organisations should review their ISTA program periodically (Herold, 2010; Whitman, 2008; Wilson & Hash, 2003; Wright, 2005). The review will assist organisations to continually improve their ISTA program (Whitman & Mattord, 2008). The practice of reviewing the ISTA program consists of two activities: (1) measure the effectiveness of the program and (2) Update ISTA’s materials.
Practice 6-Activity 2: Measure the effectiveness of ISTA program
There are several ways the effectiveness of an ISTA program in an organisation can be measured (Whitman & Mattord, 2008). First, feedback needs to be collected from employees about the ISTA program. It can be obtained by various means such as evaluation forms/questionnaires, focus groups and selective interviews. Second, employees should be observed to find out whether they are following the recommended security procedures. Third, the number and the type of information security incidents that occurred before and after ISTA program was conducted.

Output from measuring the effectiveness will outline the strengths and weaknesses of the ISTA program in place and, therefore, enable the organisation to improve their ISTA program by revising the plan and updating the materials. In addition, any change in the ISP as a result of new risk assessment will lead to a change in the organisation’s need for ISTA.

Practice 6-Activity 2: Update ISTA’s materials
Continual update of the security policy to mitigate security risks should lead to a change in the needs for the ISTA program (Kruger & Kearney, 2006; Lebek et al., 2013; PCI, 2014). The change in the needs should lead to a change in the ISTA plan and materials. Therefore, the organisation should review the plan and materials and update them. It is important to note that both this task and the previous one provide recommendations or input for the development stage. In other words, the input will be used for redevelopment of the ISTA program.

7.4 Data Analysis and Findings
As described in Section 3.5.1 semi-structured interviews were conducted to refine and validate the preliminary framework. A total of thirty-four information security experts were interviewed in this research project (See Table 3-1). Six interviews were conducted to validate the framework of ISTA practices while the remaining twenty-eight interviews that focused on other areas of ISMP that also mentioned the ISTA practices but not in great detail. The data obtained from the interviews was analysed as outlined in Section 3.6. Table 7-6 provides details of the ISTA practices that have been identified from the coding and analysis process and the number of participants who supported the practices from the area focused interviews and interviews on other ISMP areas.
The remainder of this section presents the key findings and evidence from the empirical study. Supporting quotes will be from the six interviews that focused on ISTA.

### 7.4.1 The Development Stage

This section presents the key findings and evidence related to practices undertaken to develop the ISTA program. Four practices were identified by the interviewees as an important practice to develop the ISTA program: (1) Conduct a needs assessment for the ISTA program, (2) Establish ISTA development team, (3) Create a ISTA program plan and (4) Develop ISTA materials. The following subsections discuss these three practices.

**ISTA-Practice 1: Conduct needs assessment**

The need assessment for the ISTA Program aims to identify what areas/topics employees need to be aware of and the people who should be given security awareness, training or education.

In general, all six interviewees agreed that conducting a needs assessment for an ISTA program is an important practice. Also, six interviewees from other ISMP areas mentioned this practice. Within the scope of what the literature describes as part of conducting a needs assessment practice, interviewees outlined one key activity, which undertaken in organisations: (1) Identify inputs for the needs assessment. The remaining of this subsection presents evidence related to this activity.
Practice 1-Activity 1: Identify inputs for the needs assessment

All six participants indicated that the needs for ISTA can be identified using inputs from policy, incident reports, risk assessment, threat intelligence, and users’ feedback. For instance, P17_Mng_ISTA stated:

“There are numerous inputs that go into it. It's, one, understanding the threat landscape: what is currently happening or what's being advertised. There's also a component around what incidents have we seen in the past, be they to our organisation or to other industries or organisations. We also take into account new technologies that are impacting consumers and our staff. Then, we also look at what user feedback we are receiving. If people are actually saying that these are their concerns--these are their issues, we'll also feed that into it, as well. Then, also, the strategic direction of where the ISO wants to build capability. That will really dictate more or less the key areas. User input is key, regulatory environment obviously is another element.”

Additionally, several examples were provided by interviewees on how incidents were used for awareness purposes within an ISTA program. P15_Mng_ISTA explained that if there is a phishing attack on the organisation, this presented an opportunity to raise the employees’ awareness on this type of threat.

ISTA-Practice 2: Establish ISTA development team

Only half of the participants supported this practice and reported that they have a dedicated team for ISTA. From the remaining twenty-eight participants, four mentioned that they have an ISTA team during the discussion.

Although not all the participants in the ISTA focused interviews supported this practice, it was indicative from the discussion that in the organisations where a dedicated team for ISTA does not exist, an ad hoc team is established to manage the ISTA program. Only one key activity was reported as part of this practice: define roles and responsibilities.

Practice 2-Activity 2: Define roles and responsibilities

All participants generally agreed that the delegation of roles and responsibilities around ISTA is a key activity. The participants reported that several activities are undertaken to manage ISTA, including creating the training material, publishing it and ensuring that employees complete the training. In response to the question ‘who is responsible for managing the ISTA program in your organisation?’ Half of the participants stated that they have formal team which consists of three to four members. P15_Mng_ISTA states:
“There is a team responsible for security training and awareness. They have the responsibility to create the training material, publishes it on the portal CBT learning portal. And track completion.”

While the remainder of the participants explained that there is no informal team for ISTA and responsibilities for ISTA may be (1) undertaken by members of the organisation’s security team, (2) outsourced to third party and (3) delegated to learning and development unit if there is one in the organisation. For instance, P13_MngISTA reported:

“At my last organisation, [Bank] we had a team called learning and development team, they were responsible for managing all CBT or classroom based training. [...] but in my current organisation, we don't have learning and development unit. What we [security team] do is that we develop the program, we put that policy as part of HR package that becomes HR policy.”

P13_MngISTA further provided justification for not having a dedicated team in his organisation. He stated that because the size of his organisation is small, they don’t have a dedicated team for ISTA.

“That is probably more of a reflection of the size of our organisation that we are not quite big enough to have a dedicated team of personnel dedicated to this task.”

P13_MngISTA

In terms of roles, interviewees have named several roles for developing and designing ISTA materials, delivering the program and coordinating between stakeholders in the process. For example, P4_Mng_Policy mentioned that every department in the organisation “nominate” someone to coordinate awareness activities and identify the needs for ISTA within his department. The participants also mentioned stakeholders such as communication officers, human resource managers are heavily in the management of ISTA program. Senior managers also play a vital role in the oversight involves and supporting the ISTA program and its practices.

ISTA-Practice 3: Create an ISTA program plan

In general, all six interviewees stated that they develop a plan for ISTA. They reported three activities organisations undertake to plan for ISTA program. These activities include: (1) Define goals and objectives of the program, (2) Identify target group, and (3) schedule ISTA program activities. Following is a discussion on data related to activities conducted to develop a plan for the ISTA program.
Practice 3-Activity 1: Define ISTA program goals and objectives
All participants discussed the importance of defining goals and objectives for ISTA. P15_Mng_ISTA stated:

“we set objectives for the short campaigns for example, security and fraud week is develop to achieve specific objectives. We also have a very high-level objectives that we’d like to achieve for the overall security awareness program”

Four participants also indicated that one of the key elements of an ISTA plan is to identify the level of awareness you want to achieve. They further added that during needs assessment, the organisation will be able to identify the organisation’s requirements for ISTA. These needs will be outlined in the plan as goals and objectives to be achieved by the development of an ISTA program.

Practice 3-Activity 2: Identify target group
All interviewees indicated that their organisations group employees according to their roles and responsibilities. Then, they develop an ISTA program to fulfil the needs of each group. For example, P13_Mng_ISTA stated that,

“In my organisation, there are three kinds of training and awareness program: one for executive management, the second type of security training and awareness is general awareness message for all employees from all the departments and the third type is target specific group awareness.”

All interviewees agreed that the ISTA program should be tailored to address the needs of each target group. In other words, different types of ISTA should be designed. As P16_Mng_ISTA states:

“There is no one size fits all approach. [...] we need to tailor our awareness campaigns depending on the stakeholder group that we are dealing with.”

Each type should have its own characteristics in terms of the content, length/duration, frequency, and delivery methods required to meet the needs of different groups in the organisation. For instance, the ISTA for executive level management would be short and concise.

Practice 3-Activity 3: Schedule ISTA program activities
One of the key activities that have been reported by all interviewees as part of the ‘create an ISTA program plan’ is to develop a schedule for the ISTA activities.

“We do have a formal schedule for awareness training” P16_Mng_ISTA
“one of the main elements of our security training and awareness plan is the
schedule. Delivery timeline that have list of training and awareness initiatives we
are planning to implement”  P15_Mng_LISTA

P17_Mng_LISTA and P18_Mng_LISTA provided a detailed explanation of their schedule of their
annual training that is delivered via computer based training (CBT).

“Our timeline around CBT basically have things like when it should be update and
available to our employees, sending email to managers and group leader to notify
them the CBT is available so they encourage their employees to take the training.
We also have certain dates to check completion rate and send emails to remind
people who did not complete the training. In addition, audits and review process
have specific dates in our plan” P17_Mng_LISTA

From previous quotes, it is obvious that schedules have two different levels. A general level
schedule for all the activities the organisation is planning to conduct and a very specific and
detailed schedule that focus on the management of each ISTA initiative.

**ISTA-Practice 4: Develop ISTA materials**

It was generally agreed among all interviewees that developing ISTA materials is an essential
practice which they undertake as part of their role in managing ISTA. According to the
participants, there three key activities that need to be performed during the development of ISTA
material: (1) Determine the security message, (2) Select optimum message delivery mechanism,
and (3) Construct the training and awareness materials.

**Practice 4-Activity 1: Determine the security message**

All the participants stressed the importance of determining the security message which they
want to convey to the organisation’s employees. For example, P16_Mng_LISTA states

“So in designing the awareness material they're looking at what message are you
trying to bring across.[…] The second thing is how you present that message?”

The message is derived from the needs which have been identified previously from the security
policy or an incident. However, during the practice of designing the material the message is
more focused. For instance, the message may focus on setting passwords or not clicking a link
in phishing emails.

**Practice 4-Activity 2: Select optimum message delivery mechanism.**

The delivery methods used to deliver the training and awareness vary according the message
and the target group. Examples of delivery methods include email, computer-based training
(CBT), classroom training and posters. Participants suggest that the use of a mixture of delivery
techniques is an effective way to convey training and awareness messages. For example, P17_Mng_ISTA states:

“*We have our newsletter which is also via our email. [...] We do use some poster materials, so there are several channels depending on what it is that we are trying to achieve*” P17_Mng_ISTA. Likewise, P16_Mng_ISTA also offers that numerous techniques are used: “*It's a program that should run throughout the year. With all sort of component such as flyers souvenirs, workshops, small groups, you can have different messages targeted to different people*”

**Practice 4-Activity 3: Construct the training and awareness materials**

This activity involves the actual creation, preparation and designing of the training and awareness materials. Participants reported that once they determine the message and the delivery methods, they start the creation of the materials and prepare. The participants reported three main approaches to the creation of the material:

First, the security managers create the materials themselves. P1_Mng_Policy stated that she develops the power point slides and design posters.

“I prepare the ppt with more examples and scenarios and design posters” P1_Mng_Policy.

Second, they use pre-existing materials that fits into the message they want to deliver. For examples, P13_Mng_ISTA reported that

“*we using some good videos which is available by Australian government for Australian government sector*” P15_Mng_ISTA.

Third, the material is created by an external vendor where the security manager provide input to the process. P13_Mng_ISTA stated that

“*we use an external vender who specialized on training and awareness. We give them our existing policy and the key messages we want to deliver.*”

The participants stated once the preliminary materials are developed, it will be shared with representative stakeholders to review and provide feedback. For instance, P15_Mng_ISTA and P17_Mng_ISTA stated that they have stakeholders’ involvement during the development of ISTA materials.

“*we create the material and send it to the stakeholders, and then we ask them to provide feedback on the materials, revise it, and publish it.*” P15_Mng_ISTA

Once the feedback is received and incorporated, the material will be ready to be used as part of various types of the ISTA program conducted in organisations.
7.4.2 The Implementation & Maintenance Stage

This section presents data related to practices undertaken to implement and maintain the ISTA program. One key practice was identified by interviewees as part of this stage: Conduct the ISTA program. Following subsections discuss conduct ISTA program practice and activities undertaken as part of this practice.

ISTA-Practice 5: Conduct ISTA

The practice was supported by all six participants in the ISTA focus interviews and twenty-one out of the remaining twenty-eight participants have also mentioned this practice during the discussion of other ISMP areas.

Several activities were identified as part of ‘conduct the ISTA program’: activities: (1) Conduct mandatory training for all employees, (2) Conduct ISTA for specific groups, (3) Conduct an intensive awareness campaign, and (4) conduct ongoing awareness messages.

However, some interviewees reported that they undertake all four activities while other only conduct one or two activities. Organisations differ based on the size, availability of resources and the maturity level.

Practice 5-Activity 1: Deliver mandatory training for all employees

All the interviewees indicated that they conduct mandatory security training for all employees. The most common way to conduct this training is through computer based training (CBT). Employees use their credentials to login to the training portal, then go through the automated training.

“We have mandatory online training that everyone must complete. Part of that includes a segment on information security that everyone must complete and must pass.” P16_Mng_ISTA

Computer based training enables organisations to obtain statistics of completion rates, and where employees fail to understand the training. This is extremely useful to fulfil compliance requirements by showing managers and, internal and external auditors, statistics of the number of employees who completed the training and how many times they have undertaken that type of training.

Participants argued that CBT within an ISTA program has several drawbacks. First, the lack of human interaction means that if an employee has a question or requires clarifications about the training they will not have the chance to ask. Second, CBT does not suit everyone’s preferences
and learning styles. Some people prefer face to face contact where they get the chance to learn and socialize instead of setting in front of a screen. Third, statistics of completion are poor indicators of the awareness level of employees. Last, three of the participants stated that CBT is difficult to manage and maintain.

**Practice 5-Activity 2: Deliver training for specific groups/teams**
The second activity that is conducted by organisations, is ISTA for specific groups. For example, specific training and awareness conducted for managers, or employees of a particular department, or a team in the organisation. As P13_MngISTA points out, this is usually done as training session or briefing:

> “We have focused security awareness program for specific employees. For example, in my job at the Banking sector, we had specific ISTA programs for call center people that is not applicable for all employees, it is only applicable for the call center.”

The participants asserted that the main advantage of this type of ISTA is that it is direct and specific to address the needs of a particular group.

**Practice 5-Activity 3: Conduct an intensive awareness campaign**
The third activity as part of conducting an ISTA program is to conduct an intensive awareness campaign over a day or a week. For example, some organisations conduct a security awareness week. P16_MngISTA and P17_MngISTA stated that they have security awareness weeks within their organisations.

> “we have an information security week where we have a slogan for the week: ‘Maybe security is not complete without you’. We have banners placed all over the organisation. We have flyers, posters, make souvenirs, we have t-shirts, face caps, bags, different things that have security’s slogan.”

> “we have an annual security and fraud awareness week. That's run right across the group. This year, we reached over 30 geographic locations and had several events in those locations and leadership support.” P16_MngISTA

The participants argued that conducting an intensive and focused ISTA program is very useful in getting the organisation’s employees interested and motivated about security issues.

**Practice 5-Activity 4: Provide ongoing awareness messages**
All interviewee’s state that they have an ongoing awareness campaign where awareness messages are presented throughout the year in the form of emails, posters, screensavers, banners, pop up messages and newsletters … etc. P13_MngISTA states:
"every month or quarter we give them reminder awareness messages. We call it snapshot awareness, which comes in the form of email which is sent to them, a nice poster with key messages whenever we see new threats in the market”.

The participants argued that conducting an awareness campaign throughout the year is essential to provide a constant reminder for employees about good security practices, as well as warning about emerging threats.

7.4.3 The Evaluation Stage

This section discusses the findings and evidence related to the review and evaluation of ISTA programs. The evaluation stage has one key practice which is to review the ISTA program periodically.

ISTA-Practice 6: Review ISTA program periodically

There was a consensus among the all interviewees that the ISTA program should be reviewed annually or bi-annually. Interviewees reported two key activities. These activities are: (1) evaluate the effectiveness of the ISTA program, and (2) Update the ISTA program materials.

Practice 6-Activity 1: Measure the effectiveness of the ISTA program

There is agreement amongst participants on the need to measure the effectiveness of the ISTA program. Participants suggested several effectiveness checking techniques:

(1) measuring security awareness indications (i.e. the number of reports of security incidents and number of incidents from threats addressed in the ISTA program),

“More Number of calls show that people are understanding risks and they are reporting it.” P15_Mng_ISTA

(2) testing the knowledge of employee pre and post training attendance,

“We perform Ad Hoc testing to check whether a person has understood and the policy.” P1_Mng_Policy

(3) performing phishing simulations,

Organisations may hire consultants to “send fake spam or phishing email or malware to the organisation network. It does not impact it, but tests how employees react to this test. It is just to check the implementation of security training and awareness program in the organisation” P17_Mng_ISTA. The aim of such exercise is “to check [whether] (1) the organisation’s system or control detect it or not? (2) what does the users do, click on it or report it? If they are aware
of this risk and they have understood they will not click and report it to helpdesk.”
P17_MngISTA

(4) conducting internal and/or external audits for the ISTA program, and

“Every training undergoes an internal audit every year, so every year a department
is getting audited by one of the information security analysts in my department.
Every three years, they are getting audited by me.” P1_Mng_Policy

(5) collecting feedback from stakeholders.

Employees’ feedback is also important indication of the effectiveness of the program.
Therefore, P15_Mng ISTA stated that they capture qualitative feedback from the stakeholders
about the program.

**Practice 6-Activity 2: Update the ISTA program**

All interviewees stated that they periodically review and update the ISTA materials. For
instance, P4_Mng_Policy states:

“we constantly update our program, create new scenarios and send it to them,
change the colour and the look put new cartoon, creates new message out of it
because threats keep changing out there. Threats are not the same threats that are
here today they will not be here 10 years later”

This is crucial to ensure materials are up-to-date to achieve the goals of the program. Any
change in security policy and in the risk landscape should result in changing ISTA materials
and plans.

All participants stated that they review the content of the ISTA program every year and
incorporate any change in the organisation’s security policy and risk assessment. The review
will provide input to the development stage.

**7.4.4 Summary of the findings**

This section discusses changes to the proposed framework of ISTA management practices as a
result of the empirical refinement and validation via semi-structured interviews with
information security experts. The empirical data has provided rich understanding of the
management process of ISTA in organisations which led to several changes to the preliminary
framework. These changes include adding new activities to practices, and renaming the
practices and activities, Table 7-7 presents the refined framework of ISTA management
practices.
In the development stage, although, there was no change in the practices, more in-depth understanding was obtained on the needs assessment, the establishment of ISTA development team, and the development of the ISTA materials.

In the implementation and maintenance stage, the practice of conducting the ISTA program had originally been two activities. However, four new practices were added that describe how the ISTA program is conducted in organisations.

In the evaluation stage, although, there was no change in the practices, more in-depth understanding was obtained especially on how organisations measure the effectiveness of their ISTA program.

### 7.5 Final validation

As explained in Section 3.5.2, an email was sent to each of the six participants who were interviewed in the first empirical study, to provide feedback on the framework and comments on whether the practices and key activities are comprehensive. Only four participants responded with their comments and feedback on the framework.

Overall the participants were satisfied that the ISTA framework reflects the practices and activities undertaken in organisations to manage the ISTA program. The participants provide

<table>
<thead>
<tr>
<th>Stage</th>
<th>Practice</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Conduct needs assessment</td>
<td>Identify inputs for the needs assessment</td>
</tr>
<tr>
<td></td>
<td>Create an ISTA program plan</td>
<td>Define ISTA program goals and objectives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify ISTA program target group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schedule ISTA program activities</td>
</tr>
<tr>
<td></td>
<td>Establish ISTA team</td>
<td>Define roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>Develop ISTA materials</td>
<td>Determine the security message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select optimum message delivery mechanism</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Construct ISTA program materials</td>
</tr>
<tr>
<td></td>
<td>Conduct the ISTA program</td>
<td>Deliver mandatory training for all employees</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deliver training for specific groups/ teams</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Conduct intensive awareness campaign</td>
</tr>
<tr>
<td></td>
<td>Review the ISTA program</td>
<td>Provide ongoing awareness messages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Measure the effectiveness of the ISTA program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update the ISTA’s materials</td>
</tr>
</tbody>
</table>
several suggestions on the framework that were originally addressed in the description of the practices and key activities of the ISTA framework. For example,

“One item that may be worth considering as part of ISTA development is a step to validate (test) the effectiveness before general implementation. It is really important to check that it meets the defined requirements (objectives) before a broader roll out to the constituents. This also affords an early opportunity to solicit feedback and refinement too.” P17_Mng_ISTA

In the ‘Practice 4-Activity 3: Construct the training and awareness materials’ the ISTA development team seeks feedback from stakeholders and incorporate the feedback to refine the material and ensure it is ready for the implementation.

Another comment was that

“During the Development Stage, you must define the success criteria (KPI) which will be used during the Stage 4 i.e Evaluate, these KPI are developed based on the result of your assessment during Develop Stage” P13_Mng_ISTA

This is part of the activity ‘Define goals and objectives for the program’. A clear and achievable goals and objectives of the ISTA program can serve as a key performance indicators (KPI). During the evaluation stage the ISTA team will check if the program’s goals and objectives are achieved.

7.6 Discussion

The analysis of the empirical data enabled a rich understanding of the managerial practices of ISTA undertaken in organisations. The main contribution of this study is the identification of the set of activities that are required to develop an ISTA program and the extent to which these activities are implemented in organisations. The set of key activities are comprehensive and exhaustive. No other activities were identified. The findings have provided an insight of how these activities have been institutionalized and how well they have been resourced.

7.6.1 Towards a formal approach to the Implementation of ISTA activities

The findings have provided evidence that can be used to identify the differences between the implementation of ISTA activities in organisations. Respondents from large organisations reported that they formally implement the set of activities where training and awareness takes place. Whilst in small organisations, because of a lack of resources (i.e they do not have dedicated team for ISTA) training and awareness activities are dealt with more informally and occasionally may not be done at all.
Conducting a needs assessment for training and awareness is one of the key practices that has been reported by the participants. The findings of this study provided insight on how this practice is conducted in organisations. Participants from large organisations stated that they use security policy, recent risk assessment and incident response reports to identify the requirements for the ISTA program. While respondents from small organisations reported that they undertake this practice, they stated that it is done in an ad-hoc manner using only the security policy as opposed to the various inputs used by large organisations.

From the security and awareness program planning perspective, the extent to which planning is formalized depends on the circumstances and the characteristics of the organisation. In large organisations, there are thorough planning activities, which cover long term (strategic) and the short term (tactical) aspects of ISTA. In small organisations, there is some planning, however, it is neither comprehensive, nor formal. Planning covers a few high-level elements such as scheduling of activities. This variation can be contributed to the maturity and size of the organisation as well as aspects of management support and the availability of resources (including time and personnel).

In terms of conducting the ISTA program, while participants from small organisations stated that they only conduct mandatory training using computer based training (CBT), participants from large organisations reported that several training activities were conducted (see the section on conduct ISTA). The difference in the extent of the implementation of conducting training and awareness can be contributed to the lack of resources and the low awareness of the role of ISTA in protecting the organisational information assets in smaller organisations. The literature suggests that to increase the effectiveness of ISTA, organisations should implement the program using various methods, not just CBT (Kim, 2014). The use of many delivery methods increases the effectiveness of ISTA as it considers the preferences and the learning style of different employees in the organisation. Subsequently, the selection of the delivery methods should take into consideration the type of message and the intended target audience (Abawajy, 2014).

The findings of this study show that organisations recognize the importance of evaluating their ISTA program. Respondents from large organisations reported that they employ various methods to measure effectiveness of ISTA and to monitor the changes to employee behaviour. However, respondents from smaller organisations indicated that they depend on training statistics generated by CBT to track the effectiveness of training and awareness. This is done mainly to meet compliance and regulatory requirements not to measure the effectiveness of the
program. That means in these kinds of organisations that their ISTA program may not be optimal.

7.6.2 Developing an effective ISTA program

The study participants provided insights and recommendations on strategies to create an effective ISTA program through focusing on motivating aspects. These recommendations include: motivate employees through effectively communicating the purpose of the ISTA program, building trust and good relationships with stakeholders, engaging stakeholders in managing ISTA activity through providing feedback, and relating the ISTA messages to the employees’ private life. The participants also stated that by relating information security to the employees’ personal life motivated them about information security. To the best of our knowledge, using personal life to motivate has not been reported in the literature.

Several recommendations were also provided by the participants to overcome the challenge of competition with other organisation training initiatives for employees’ attention. First, organisations should consider using multiple delivery methods and try to be creative and innovative in the way the organisation delivers their ISTA program. Second, organisations should reduce content and increase motivation. Third, organisations should focus on employees who deal with sensitive information and processes. These recommendations have been reported in the current literature. However, the findings of this study extend the literature by suggesting that organisations should look at consolidating training across organisational functions to reduce the number of training courses and to reduce the competition for employee’s attention. For example, the induction training program for new employees should embed basic information security training. This requires constant liaison and communication between HR people and the information security personnel who are responsible for the security awareness and training program. This suggestion is in line with Puhakainen and Siponen (2010) recommendation to integrate the ISTA program with normal business communication of the organisation.

The findings of this study show that current techniques and methods employed in organisations to measure effectiveness of ISTA can only provide an indication, but not a comprehensive assessment, of the effectiveness of the ISTA program. For example, the study respondents stated that the number of reports of security incidents around threats addressed in the ISTA program is used as an indication for the level employee’s security awareness. However, the number of security incident reports does not necessarily reflect the extent to which the ISTA program is effective in imparting an awareness of risk for two reasons. First, ‘incidents’ are variably defined
and that not every event is an incident. Second, increases in incident reports may occur as a result of an increase in the number or sophistication of attacks. Therefore, it is still unknown to organisations how effective their ISTA programs are in changing employee’s behaviour and how much they should invest on ISTA to be able to get an effective outcome. This is still an elusive goal for organisations to achieve. The findings suggest that the organisations should use a combination of effectiveness checking techniques to enable them to measure the effectiveness of their ISTA program. It is also recommended that organisations develop their own success metrics to measure their ISTA program.

7.7 Summary
This chapter presented the development and refinement of the ISTA management practices framework. It started by providing an overview of the literature on the ISTA domain, then a framework was developed based on rigorous and comprehensive review of the literature. The refinement and validation of the proposed framework was also presented. The chapter ended with a discussion of the findings from the empirical data and the contribution. The next chapter will present the development of the information security incident response management framework.
Chapter 8 INFORMATION SECURITY INCIDENT RESPONSE MANAGEMENT PRACTICES

8.1 Introduction
The previous chapter presented the development and validation of the information security training, and awareness (ISTA) management practices framework. This chapter describes the development and validation of the framework of the managerial practices of information security incident response (ISIR). The aim this chapter is to: (1) provide a comprehensive overview of the management practices of ISIR process, (2) develop a practice-based framework, (3) refine the proposed framework, and (4) discuss the findings and contributions of the proposed framework to the ISM literature.

This chapter is organised as follows. Section 8.2 provides an overview of existing incident management literature, highlighting related research gaps and deficiencies. Section 8.3 presents the proposed framework of ISIR management practices. Section 8.4 presents empirical data from expert interviews that have been conducted to refine the proposed framework. Section 8.5, presents the analysis and findings from the follow up interviews which were conducted for final validation of the framework. Section 8.6 discusses contribution and implications of the proposed framework for ISIR management practices, and Section 8.7 provides a summary of the chapter

8.2 Literature Review
Information security incident response is a critical security function in organisations (Ahmad, Maynard, et al., 2015; Baskerville, Spagnoletti, & Kim, 2014). It refers to the organisation’s procedures to anticipate information security incidents, plan and prepare for, detect, contain, eradicate, recover from incidents, and identify lessons learnt from incident responses (Ahmad, Hadgkiss, et al., 2012). It aims to enable organisations to respond to security incidents
effectively, which will minimise the effect of security incidents on the systems and the overall business functions (Ahmad, Maynard, et al., 2015; Bowen et al., 2006; Fowler, 2016).

Due to the increase in the number of information security incidents and the significant consequences on business processes, the ISIR function has gained considerable attention from academics and practitioners. Much of the research in the ISIR area focuses on improving the organisation’s capability to respond swiftly to security incidents. Several international standards and guidelines (SANS, ISO 27035, NIST 800-61) have been developed to provide guidance for organisations to prepare and respond effectively to information security incidents.

Subsequent research investigates individual aspects of the incident response lifecycle. For example, several studies focused on the planning and preparation for incidents (Caldwell, 2012; Line et al., 2014; Tan, Ruighaver, & Ahmad, 2003), while others (Ahmad, Maynard, et al., 2015; Gerd Van Den Eede, Willem J. Muhren, & Walle, 2008; Jaatun, Albrechtsen, Line, Tøndel, & Longva, 2009; Shedden, Ahmad, et al., 2010; Tøndel, Line, & Jaatun, 2014) investigated aspects of learning from incidents and how lessons learned can be incorporated into other ISM functions.

A number of studies focused on issues relating to the incident response team such as the structure of the team, who should be involved in the team, responsibilities, communication between teams and other stakeholders, the effectiveness of the team and challenges faced by the team (Ahmad, Hadgkiss, et al., 2012; Chen et al., 2014; Killcrece, Kossakowski, Ruefle, & Zajicek, 2003a; Ruefle et al., 2014; Steinke et al., 2015; Sundaramurthy, McHugh, Ou, Rajagopalan, & Wesch, 2014). The following sections discuss ISIR management in the literature.

**8.2.1 Review of existing ISIR approaches and guidelines**

Several standards and guidelines have been proposed to assist organisations in planning and preparing for information security incidents. A structured approach to information security incident management was proposed by ISO/IED 27035 “information security incident management” and NIST Special Publication 800-61 (Grance, Kent, & Kim, 2004) “Computer Security Incident Handling Guide”. ISO/IED 27035 and NIST Special Publication 800-61 are the main standards in the domain. They include practices relating to: 1) planning and preparing for incident response, 2) responding to a security incident, and 3) reviewing and improving how an incident has been handled.

SANS (Northcutt, 2003), ENISA (ENISA, 2010a), and FCC (US Federal Communication Commission, 2001) also offer guidelines for incident response, which are similar to the approaches proposed by ISO/IED 27035 and NIST Special Publication 800-61. While ENISA guide “Good Practice Guide for Incident Management” does not include planning preparation practice, SANS “Incident Handling Step-By-Step” dedicates nearly half of the guide to the planning and preparing phase of the ISIR process. SANS stated that a well-prepared organisation will be able to “act quickly and effectively when a computer security incident occurs” (p.16). FCC “Computer Security Incident Response Guide” consists of six stages: preparation, identification, containment, eradication, recovery and follow-up. Carnegie Mellon Software Engineering Institute offers a “Responding to intrusions” guide (Kossakowski, Allen, Alberts, Cohen, & Ford, 1999), State of the Practice of Computer Security Incident Response Teams (CSIRTs) (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003b) and “Handbook for Computer Security Incident Response Teams (CSIRTs)” (West-Brown, Stikvoort, Kossakowski, Killcrece, & Ruefle, 2003). “Responding to intrusions” describes a three-phase approach for security incident management: prepare, handle and follow-up whereas the CSIRTs is comprehensive guide for setting up an ISIR team.

The ISIR process proposed by the abovementioned standards and guidelines can be summarised into three main phases: planning and preparation phase, incident response/handling phase and post incident/follow-up phase. The remaining of this section discusses common practices within each phase of ISIR management.

- The planning and preparation phase

The planning and preparation phase is considered the most important phase in security incident response as it enables organisations to respond quickly and effectively to security incidents (Bowen et al., 2006; ENISA, 2010a; Kibirkstis, 2009; Tøndel et al., 2014). The planning and preparation phase involves developing an ISIR approach, gaining support from top management, developing an ISIR management scheme, and updating security policy and risk analysis. The planning and preparation phase also includes establishing an information security incident response team (ISIRT) and conducting awareness and training related to security
incident management (Caldwell, 2012; Cusick & Ma, 2010; Tan et al., 2003; Werlinger, Muldner, Hawkey, & Beznosov, 2010).

It is important to note that some of the practices within the planning and preparing phase are related to the establishment of an information security program (ENISA, 2010a). This encompasses doing a risk assessment, developing security policy and implementing security controls, conducting training and awareness (Caldwell, 2012; Goldes et al., 2017; Line et al., 2014).

A recent study by Line et al. (2014) found that although some information security incident response standards such as ISO/IEC 27035 recommend practices related to planning, organisations do not undertake planning practices. A total of nineteen participants from six organisations in the report said their organisations either does not have a plan or the plan is not well developed, rather it is left to the employees to figure out what to do in regard to a ISIR. This finding is consistent with the conclusion of an earlier study by Tan et al. (2003) showing that there are inadequate planning activities for incidents in organisations. While the importance of preparing and planning for incidents is well recognised in both practitioner and academic literature, the planning is not practised in organisations, which might indicate that organisations do not have sufficient guidance on planning and preparing for incidents. Moreover, the technical view of the process also contributes to the lack of planning activities for incidents (Tan et al., 2003).

- The incident response phase

The second phase in the process of security incident management is the incident response phase (Kibirkstis, 2009; Northcutt, 2003). This phase is triggered by the occurrence of a security incident. Activities with the incident response phase include detecting and reporting security incidents. It also consists of practices performed to assess security incidents and take all necessary steps to respond to them. These practices include detecting, containing, eradicating, and recovering from an incident (DePaul University security team, 2002; ENISA, 2010a; Northcutt, 2003). These practices are mainly technical (Fowler, 2016; Hove, Tarnes, Line, & Bernsmed, 2014; Shedden, Ahmad, et al., 2010)

- The Follow-up phase – Post incident phase

The final phase is the follow-up phase (ENISA, 2010a; Hove & Tårnes, 2013; ISO/IED 27035, 2011). This phase includes identifying lessons learnt from the ISIR process (Cooke & Rohleder,
Lessons learnt encompasses conducting a review and analysis of the incident in order to identify improvements needed to the security program (i.e., implementing extra controls). ISIR management is an iterative process where the follow-up phase will provide feedback to the first phase, planning and preparation (Cooke & Rohleder, 2006; Shedden, Ahmad, & Ruighaver, 2011). This will ensure that organisations are always prepared.

The literature suggests that discussion within the ISIRT during the follow-up phase is limited to the technological aspect of information security rather than a managerial strategic management point of view (Ahmad, Hadgkiss, et al., 2012; Ahmad, Maynard, et al., 2015; Tøndel et al., 2014). Further, the learning from an incident to incorporate the lessons learnt is very limited and usually informal and ad-hoc (Ahmad, Hadgkiss, et al., 2012; Shedden, Ahmad, et al., 2011; Webb, Ahmad, Maynard, Baskerville, & Shanks, 2017).

Overall evaluation of the ISIR process is not performed as the focus is placed on individual incidents. The evaluation of the entire ISIR process receives little attention in the literature. The evaluation within existing ISIR approaches focuses on providing recommendations to improve security systems (recommended controls are mainly technical). However, suggestions to improve the ISIR process are not emphasised. Some existing approaches offer very abstract level suggestions for updating the policy and procedures, and the communications plan. Ahmad, Hadgkiss, et al. (2012) argue that there is a lack of attention given to the learning aspect of incident response and post incident function.

Shedden, Ahmad, et al. (2011) conducted a series of focus groups and interviews with security and forensics experts to study issues relating to ISIRT. Shedden, Ahmad, et al. (2011) argue that ISIR approaches proposed by best practice guidelines present the learning process as a structured and formal process. Tacit knowledge and informal learning is not considered. The authors suggested that informal learning should be considered to increase the effectiveness of the learning process. Subsequent study by Ahmad, Hadgkiss, et al. (2012) investigated challenges facing ISIRT that impact on the overall security function. The case study uncovers issues such as disparity in incident response approaches, lack of a formalised information dissemination process and focus on technical learning over policy and risk. Ahmad, Hadgkiss, et al. (2012) propose a double-loop incident learning system model to overcome the identified challenges from the case study.
8.2.2 Information Security Incident Response Team (ISIRT)

There is a consensus in the literature on the importance of establishing an ISIRT. Once an incident is detected, the team gets deployed to perform incident handling practices. According to AS/NZS ISO 18044 the ISIRT plays a central role in the process. ISIRT duties include “assessing, responding to and learning from information security incidents, and providing the necessary co-ordination, management, feedback and communication” (p.20).

The literature discusses various issues concerning the establishment of the ISIRT such as the structure, the size, members, roles and responsibilities, required skills and knowledge, communication and collaboration between relevant stakeholders and the team, and the effectiveness of the team (Steinke et al., 2015; Sundaramurthy et al., 2014). In terms of the structure of ISIRT, ISO 18044 states that in most cases “the ISIRT will be virtual team, with a senior leading the team supported by groups of individuals specialised in particular topic, e.g. in handling the malicious code attacks, who will be called upon depending on the type of incident concerned” (p.4). The size of the team depends on the size of the organisation. The ISIRT may include members from different parts of the organisation (e.g., Business operations, IT/Telecommunication, Audit, Human Resources and Marketing) (ENISA, 2010a). Communication with team members should be made easier by providing a list of members and their contact details (Chen et al., 2008).

8.2.3 Communication and participation of relevant stakeholders

Akin to other ISMP areas, ISIR process cannot be performed separately from the rest of the organisation’s departments. Stakeholders participation is very important in reporting a security event, and communication during a security incident (Ahmad, Hadgkiss, et al., 2012; Jaatun et al., 2009).

The literature suggests that there are three types of communications that might occur within ISIR management that serve three different purposes (Ahmad, Maynard, et al., 2015; Ruefle et al., 2014; Steinke et al., 2015). The first type is communication between managers and the ISIRT, which is used for deploying the ISIRT to assess and respond to an incident. The second type of communication occurs within the ISIRT team members during an incident to collaborate and coordinate in performing incident response practices/activities. The last type of communication takes place between general employees and the managers and ISIRT, which is used to report and investigate an incident.
8.2.4 The need for a practice-oriented framework

Several researchers recognised the need for a practice-oriented model of ISIR management (Jaatun et al., 2009; Line et al., 2014; Tøndel et al., 2014). For example, Jaatun et al. (2009) argued that “systematic incident response approaches are needed to cope with the new challenges” (p.27). Similarly, Line et al. (2014) stated that “there is a need to create a more unified approach to information security incident management” (p.47). They added that identifying the practices is valuable for seeing which practices should be strengthened and further developed in collaboration. Thus, this research aims to address the gap in the literature by developing a framework of ISIR management practice. To develop the framework, a comprehensive review of the related literature will be conducted. The proposed framework will be empirically validated through a series of interviews with security experts.

8.3 The proposed security incident response management practices framework

As described in Section 4.3.2, a comprehensive and rigorous review of the ISIR literature was conducted. The overall understanding that emerged from the review and coding process resulted in the development of a model of ISIR management practices. This section discusses the proposed framework. Table 8-1 depicts the Framework which consists of three main stages: the Development stage, the Implementation & Maintenance stage, and the Evaluation stage. Each stage consists of a number practices, each having a number of key activities.

<table>
<thead>
<tr>
<th>Table 8-1 The preliminary framework of ISIR management practices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stage</strong></td>
</tr>
<tr>
<td>Develop</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Implement &amp; maintain</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Evaluate</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Stage</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

8.3.1 The Development Stage

The development stage consists of all managerial level practices that organisations should undertake to develop incident response capabilities inside the organisations. The development stage consists of three key practices: (1) develop incident response policy, (2) develop a communication plan, and (3) establish an incident response team.

**ISIR-Practice 1: Develop incident response policy and procedures**

Developing an incident response policy and procedure is a critical practice (Bowen et al., 2006; Mitropoulos, Patsos, & Douligeris, 2006, 2007). It dictates how security incidents are reported and handled (Grance et al., 2004; Park, Ruighaver, Maynard, & Ahmad, 2012). An effective ISIR policy should consist of the following key elements:

An ISIR policy should begin with a statement of management commitment to the process (ENISA, 2010a; Ronald S Ross, 2009). This support and commitment is vital to the success of the ISIR process, as it ensures that the required resources will be allocated to the process, critical decisions made by the ISIRT will be supported, and authority will be given to undertake all the necessary steps to handle incidents (Northcutt, 2003).

Another key element of the ISIR policy is the purpose and objectives of the policy. The scope of the policy should be determined (ENISA, 2010a; Killcrece et al., 2003a; Northcutt, 2003). The scope includes all parties/stakeholders affected by the policy, when it should be applied and what the consequences are of applying it.

The ISIR policy should also include guidance on the organisational structure for ISIR management. It should also encompass definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, and the requirements for reporting certain types of incidents (Hove et al., 2014; Northcutt, 2003).

Security incident response policy should address reporting the security incident (ENISA, 2010a; ISO/IEC18044, 2006). It should include reporting and contact forms. This is very important as it provides guideline on how an incident should be reported, to whom it should be reported, and
what tools and forms should be used to report an incident (DePaul University security team, 2002). In other words, the incident response policy should establish methods for reporting incidents.

It is recommended that the incident response policy encompasses a summary of common information security incidents, handling scenarios, reporting and resources required to address them. The resources may include people, tools and time (Fowler, 2016; Michael, 2002).

ISIR policy, like all policies, should also be distributed, communicated, and enforced (Sommestad et al., 2014). Employees’ compliance with incident response policy means that they will respond in a manner that maintains the security objectives of the organisation’s information and networked systems. See Chapter 5 for more detailed information on ISP management practices.

The development of the ISIR policy and procedures includes one key activity: develop incident classifications.

**Practice 1-Activity 1: Develop incident classifications**

Policy should provide a clear definition of the term “incident” (ENISA, 2010a; ISO/IEC18044, 2006). The definition should be clear and specific, so it sets the scope of the term. This is a very critical element that incident policy should cover as it guides the identification and the assessment of information security incidents (He & Johnson, 2017; McLaughlin, DArcy, Cram, & Gogan, 2017). Policy should also provide criteria for “prioritisation or severity ratings of incidents” that can be used to assess and prioritise an incident (He & Johnson, 2017). According to NIST an incident can be prioritised based on resources affected and the impact of the incident on the affected resources. Several classifications of security incidents can be found in the literature. For instance, DePaul University security team (2002) proposes a severity ranking system for security incidents that consists of four levels: Level One is assigned to the most severe and critical, whereas Level Four is the lowest level. Each level has specific characteristics that personnel should look for when assessing an incident, then he/she should assign a severity level according to these characteristics (Ahmad, Hadgkiss, et al., 2012; Grispos, Glisson, & Storfer, 2014; Grispos et al., 2017; Taylor, Finch, Alexander, & Sutton, 2013; Tøndel et al., 2014). The severity level will determine the procedures and resources for handling the incident (Ahmad, Hadgkiss, et al., 2012; Carver & Pooch, 2000; Hove et al., 2014).
ISIR-Practice 2: Develop communication plan

Maintaining communications with key stakeholders during the occurrence of a security incident is an essential practice (Steinke et al., 2015; Taylor et al., 2013). There are two types of communications: (1) internal communication that occurs within the organisation (between the ISIRT and the management and other employees from different departments) and (2) external communication between the organisation representative, which may be the ISIRT and other entities such as media and law enforcement agencies (K. E. Hoffman, 2013; Metzger, Hommel, & Reiser, 2011). The development of the communication plan enables effective communications which is very important for assisting organisations to identify stakeholders, determine methods of communication, and set guidelines for information sharing (ENISA, 2010a; Kibirkstis, 2009).

Developing a communication plan consists of two main activities: (1) identify relevant stakeholders, and (2) develop guidelines for information sharing of incidents.

Practice 2-Activity 1: Identify relevant stakeholders

Effective incident response cannot be performed in isolation from other departments and other organisations. Participation and collaboration of relevant stakeholders is essential for a successful ISIR process (Alberts, Dorofee, Killcrece, Ruefle, & Zajicek, 2004; Jaatun et al., 2009; Northcutt, 2003). Therefore, organisations should identify relevant stakeholders (both internal and external). Internal stakeholders include managers, business operations, human resources, IT/telecommunication, audit, marketing, disaster recovery, risk management, public relations, the legal department, and corporate communications department (ENISA, 2010a; Northcutt, 2003). External stakeholders involve other organisations’ ISIRT, law enforcement, the media, vendors, and clients (Grance et al., 2004; ISO/IEC18044, 2006).

Relevant stakeholders play a significant role in the incident response process (Chen et al., 2008; Cusick & Ma, 2010; James, 2002). Identifying stakeholders allows the ISIRT to build a relationship with those stakeholders, which encourages them to participate in the process (Sokol, 2000). It also enables organisations to communicate rapidly and efficiently with various stakeholders (Chen et al., 2008).

Practice 2-Activity 2: Develop incidents information sharing guidelines

As discussed in Section 8.2.4, the ISIRT needs to communicate with internal and external stakeholders during an incident. Communications requires collecting, analysing, and sharing
information about security incidents, which is critical, especially with external stakeholders, as sharing sensitive information with unauthorised parties may have immense consequences such as disruption and financial loss (Baskerville et al., 2014; ENISA, 2010a).

An ISIRT should have a thorough discussion with the organisation’s public affairs office, legal department, and management about information sharing with external stakeholders before an incident occurs (Northcutt, 2003). This discussion should lead to the development of guidelines for information sharing.

Organisations should also determine the methods to be utilised for information sharing (ENISA, 2010a; Steinke et al., 2015). For instance, organisations may create an internet web page that can be used to report an incident (ENISA, 2010a). In case the Internet service is not available, a printed copy of a reporting form should be used (ENISA, 2010a). Additionally, the organisation should motivate and encourage their members to report by using easy and simple reporting methods, as well as offering rewards and incentives (Freiling & Schwittay, 2007; Mitropoulos et al., 2006).

**ISIR-Practice 3: Establish incident response team**

Establishing the ISIRT is an essential practice as it aims to provide the organisation with personnel who have the necessary skills and knowledge to handle a security incident (Desouza & Vanapalli, 2005; Smith, 1994; Steinke et al., 2015; US Federal Communication Commission, 2001). The team should be defined during the development stage of the ISIR process (Prosise, Mandia, & Pepe, 2003). The role and responsibilities of the members of the incident response team should be clearly documented and communicated throughout the organisation.

Establishing an ISIRT involves four main activities: (1) determine the structure of the team, (2) define the roles and responsibilities of the team members, and (3) Schedule training for team members.

**Practice 3-Activity 1: Determine the structure of the team**

The literature suggests that there are three models for ISIRT’s structure (ENISA, 2010a; Grance et al., 2004; Steinke et al., 2015): (1) a central incident response team, (2) distributed incident response teams and (3) a coordinating team. In the central incident response team model, the organisation has one team to handle incidents throughout the organisation. This model is recommended for small organisations and large organisations with minimal geographic diversity in terms of computing resources (Ruefle et al., 2014). The distributed incident response
teams model is very suitable for organisations with large and distributed computer resources (ENISA, 2010a). It consists of multiple incident response teams; each team is responsible for handling incidents for a specific part of the organisation. Effective and efficient incident response requires strong communication among teams and consistent practices (Steinke et al., 2015).

The last type of incident response team’s structure is the coordinating team. This type of team consists of individuals with the required expertise cooperating to respond to security incidents (ENISA, 2010a). The ISIRT assists the department team to respond to an incident within their department and helps them to coordinate with other departmental teams (Ruefle et al., 2014).

**Practice 3-Activity 2: Define roles and responsibilities**

It is important to define the roles and responsibilities of ISIRT members (ISO/IEC18044, 2006; Swanson & Guttman, 1996). The overall responsibilities that the ISIRT should undertake are the incident handling lifecycle: detect, contain, eradicate, and recover from security incidents (Alberts et al., 2004; McLaughlin et al., 2017). Each of these stages has a number of activities that should be performed by ISIRT members.

The literature suggests that ISIRT from different departments within the organisation, including people from different departments, will ensure that the team includes experts from different subject areas, and is therefore capable of responding to a security incident in a timely and efficient manner (Killcrece et al., 2003a; McLaughlin et al., 2017). The participation and the cooperation of individuals throughout the organisation is a key success factor of an ISIRT (Steinke et al., 2015). The size of the team depends on the size of the organisation and the type of incident. The members should be available and easy to reach.

According to NIST 800-61 the security incident response team must have a manager, a deputy team manager, a technical lead and an incident lead. The team manager is responsible for coordinating with upper management and other stakeholders (both internal and external), resolving crisis situations, and ensuring that the team has the necessary personnel, resources, and skills. A deputy team manager should undertake the team manager roles when the manager is absent.

A technical lead has the overall responsibility for the quality of the technical work that the entire incident response team undertakes. Another important role within the incident response team is incident lead, which liaises with the handlers’ activities, collects information from the handlers,
provides updates regarding the incident to other groups, and ensures that the team’s needs are met, such as arranging for food and lodging for the team during extended incidents (Alan, 2002; ENISA, 2010a; US Federal Communication Commission, 2001).

**Practice 3-Activity 4: Schedule training for team members**

Training is an essential success factor for the ISIRT (ENISA, 2010a; Hove & Tårnes, 2013). Therefore, training should be conducted to ensure that all members of the ISIRT have the required knowledge and skills to handle incidents (Alan, 2002; Michael, 2002). Training should focus on how to respond to security incidents following recommended policy and procedures (Northcutt, 2003). Training should also focus on using tools and techniques for backup, evidence collection, and analysis, as well as other technical and managerial skills, that are required for responding to security incidents (ENISA, 2010a; US Federal Communication Commission, 2001).

McLaughlin et al. (2017) point out the lack of consensus on the set of skills that the incident response team should have to respond effectively. The disagreement in the required skills amongst researchers and professionals may contribute to the complex tasks and the lack of guidance on how incident response is performed (McLaughlin et al., 2017). Several researchers provide lists of skills including technical and soft skills (Grispos et al., 2014). Technical skills are related to key areas such as forensics, data mining, reverse engineering, configuration of countermeasures, or penetration testing (Ahmad, 2002; Elyas, Ahmad, Maynard, & Lonie, 2015; Elyas, Maynard, Ahmad, & Lonie, 2014; McLaughlin et al., 2017). Soft skills include project management and organisations skills, analysis skills, effective team building and problem solving (McLaughlin et al., 2017).

Training sessions for ISIR should provide an opportunity for the team members to discuss scenarios of security incidents, such as denial of service attacks, and determine how to handle them (Northcutt, 2003; US Federal Communication Commission, 2001). Training sessions will also assist in identifying the required resources to handle common security incidents (ISO/IEC18044, 2006). Moreover, training will help the ISIRT in understanding their roles and responsibilities in the ISIR management process (Grance et al., 2004). For more information about training in the organisation Chapter 7.
8.3.2 The Implementation and Maintenance Stage
The implementation and maintenance stage consists of one key practice which is respond to security incident. This practice consists of several activities undertaken by the ISIRT to handle security incidents. This stage is triggered by an incident being reported.

**ISIR-Practice 4: Respond to security incident**
Once the ISIRT receives a report of the incident, the team will start performing incident response activities or the incident response lifecycle (ENISA, 2010a; Grance et al., 2004; Hove & Tårnes, 2013; ISO/IEC18044, 2006; Kibirkstis, 2009). These activities include (1) Detect, (2) contain, (3) Eradicate, (4) recover from security incident, and (5) conduct review and lessons learnt meeting. These activities have been the central focus of existing incident response guidelines and standards (Line et al., 2014; Tan et al., 2003).

**Practice 4-Activity 1: Detect security incidents**
Detect security incident involves conducting assessment and analysis of an incident to determine whether the incident is a security incident (Alberts et al., 2004; Grance et al., 2004; Northcutt, 2003). It also involves investigating the incident’s scope, source, and how the incident is occurring. This information will be used by the ISIRT to deal with incident accordingly. In addition, notification of the appropriate individuals within the organisation and occasionally other organisations takes place within this activity (ENISA, 2010a; ISO/IEC 27035, 2011).

**Practice 4-Activity 2: Contain security incidents**
The aim of this activity is to limit the impact of a security incident by isolating the affected area and not allowing the incident to spread to all parts of the system (Northcutt, 2003; US Federal Communication Commission, 2001). It includes choosing a containment strategy, collecting evidence to resolve the incident, and implementing techniques to limit damage and reactionary damage from intruders (e.g., disconnection of network cables and the changing of passwords) (Kibirkstis, 2009).

**Practice 4-Activity 3: Eradicate security incident**
Eradicate security incident involves four key steps: perform corrective measures to the target environments, remove the compromised components (remove the cause of the incident), improve the network defences, and test the network vulnerabilities (James, 2002; Michael, 2002; Shedden, Ahmad, et al., 2010).
Practice 4-Activity 4: Recover from security incident
The aim of the ‘recover from security incident’ activity is to restore the system to its normal operation, validate the system, and test the system to ensure that the system is up and running. Finally, continued monitoring of the system is performed (Ahmad, Hadgkiss, et al., 2012; ENISA, 2010a; Jaatun et al., 2009; US Federal Communication Commission, 2001).

Practice 4-Activity 5: Conduct review and lessons learnt from incidents.
The ‘Conduct review and lessons learnt meetings’ activity aims to reflect on and evaluate the procedures or the activities that had been performed to handle an incident in order to minimise the possibilities of future incidents (Ahmad, Hadgkiss, et al., 2012; Gerd Van Den Eede et al., 2008; Shedden, Ahmad, et al., 2011). This result is achieved through: developing a follow-up report, reviewing incident handling activities, documenting the reviewed and revised incident handling activities, creating a follow-up report, and holding a lessons learned meeting (Kossakowski et al., 1999; Tan et al., 2003).

8.3.3 The Evaluation Stage
The evaluation stage represents all practices associated with evaluating and reviewing the management of ISIR process. Evaluating the process of handling an incident is different from evaluating the management of the whole ISIR process (Ahmad, Hadgkiss, et al., 2012).

Almost all the approaches developed by security incident response standards and guidelines involve a follow-up phase (Ahmad, Maynard, et al., 2015). The follow-up phase includes some activities to evaluate the handling activities of an incident. After a major incident has been handled, the organisation holds a lesson learnt meeting and develops a follow-up report (Ahmad, Hadgkiss, et al., 2012; Jaatun et al., 2009). However, the evaluation of the entire process of incident response has not received much attention in the literature. The follow-up phase of incident response lifecycle provides very little guidance for the organisation on the evaluation process of the entire program (Tøndel et al., 2014). It should also be noted that some practices within the follow-up phase can be applicable to evaluate the whole incident program, only if it is considered from the incident response process view rather than the incident lifecycle view. Therefore, the evaluation stage should consist of one key practice, which is ‘conduct a periodic review of security incident response capability’.
ISIR-Practice 5: Conduct a periodic review of security incident response capability

The ‘conduct a periodic review of security incident response capability’ practice consists of four activities: (1) review the incident response policy and procedures, (2) review the communication plan, (3) measure the effectiveness of the ISIRT and (4) Develop a periodic ISIR report. Although these activities are discussed in the literature within the scope of single incident, they can be undertaken in a wider context to evaluate the entire ISIR process.

Practice 5-Activity 2: Review the incident response policy and procedures

It is important to ensure that the ISIR policy and procedures are current and up-to-date (US Federal Communication Commission, 2001). The review includes assessing existing policy and procedures to determine whether the policy needs to be updated. For instance, the review may suggest updating the severity incident ranking criteria. Michael (2002) states that appropriate adjustments should be made to the incident response plan and to information security practices. No incident response plan is perfect. An organisation may be able to avoid future incidents, reduce the damage of future incidents, and get in a position to respond more effectively (Michael, 2002; US Federal Communication Commission, 2001).

Practice 5-Activity 3: Review the communication plan

As mentioned previously the ISIR communication plan is vital for effective communication and ultimately effective incident response. Therefore, review the communication plan identify possible updates is very important for an effective communication process. The update may include adding new key stakeholders and updating their roles and contacts (ENISA, 2010a; US Federal Communication Commission, 2001).

Practice 5-Activity 4: Measure the effectiveness of the incident response team

Measure the effectiveness of the ISIRT involves reviewing the incident response team’s activities. The purpose of reviewing the incident response activities is to check if the team has followed the incident response policy and procedures, determine whether team members need more training to handle a new risk source, identify the need to include new members in the team, and identify lessons learnt from responding to incidents (US Federal Communication Commission, 2001).

ISIRTs are looking for ways to evaluate their operations to not only identify strengths and weaknesses in processes, technologies, and methods but also benchmark themselves against
other similar teams (Ruefle et al., 2014). However, there are no agreed upon methods to measure and evaluate the effectiveness of the ISIRT. They further stated that various organisations are collaborating on research efforts to determine how best to measure effectiveness and identify useful metrics for tactical and strategic planning and decision making (Ruefle et al., 2014).

Much of the work in the area focused on identifying the type of questions organisations are looking to answer about their incident management capability. Different questions will require different metrics (Ruefle et al., 2014; Steinke et al., 2015). For example, effectiveness could be measured for process efficiency; performance against defined goals; success in detecting, responding to, and resolving malicious activity; preventing incident re-occurrence; and reducing incident impact (Ruefle et al., 2014).

**Practice 5-Activity 5: Develop an annual incident response report**

Develop an annual report for all security incidents that occur in the organisation, how they have been handled, resources used in the process, and lessons learnt (US Federal Communication Commission, 2001). The report is not just for one incident, but rather it is about all incidents that happened during the determined period of time. The incident response report represents the documentation part of the evaluation stage. The report should assist organisations to identify improvements for their information security program. The report will be used as an input for the development stage of the ISIR management process. Follow-up reports generated for each resolved incident can be important not only for evidentiary purposes but also for reference in handling future incidents and in training new ISIRT members (Northcutt, 2003).

**8.4 Data Analysis and Findings**

As described in Section 3.5.1 semi-structured interviews were conducted to refine and validate the preliminary framework. A total of thirty-four information security experts were interviewed in this research project (see Table 3-1). Five interviews were predominately about information security incident response management practices while the remaining twenty-nine interviews that focused on other areas of ISMP also mentioned incident response. The data obtained from the interviews were analysed as outlined in Section 3.6. Table 8-2 provides details of the information security incident response management practices that have been identified from the coding and analysis process and the number of participants who supported the practices from the area focused interviews and interviews on other ISMP areas.
The remainder of this section presents the key findings and evidence from the empirical study. This section only provides supporting quotes from the five interviews that focused on security policy.

8.4.1 The development stage

This section presents the findings and evidence relating to the management practices undertaken by organisations to develop incident response capabilities. Interviewees reported two key practices: (1) Develop incident response policy and procedures, and (2) Develop communication plan. The following sections discuss these two practices and their activities.

**ISIR-Practice 1: Create incident response policy and procedures**

All five Participants in the ISIR focused interviews reported that there are incident response policies and procedures in their organisations. It was also mentioned by six participants in the interviews about other ISMP areas. Different terms were used by the participants to refer to ‘incident response policy’. For example, P19_Mng_IR and P22_Mng_IR referred to it as a crisis management policy, while P20_Cons_IR referred to the incident response policy as an incident response methodology.

Interviewees reported three key activities that they undertake as part of the ‘Develop incident response policy and procedures’ practice. These key activities include (1) Define roles and responsibilities, (2) Develop incident classification criteria, and (3) Schedule incident response training for relevant stakeholders. Following is a discussion of these activities.
Practice 1-Activity 1: Define roles and responsibilities
As part of ‘develop incident response policy and procedures’ practice, all interviewees stated that roles and responsibilities for incident response management should be defined clearly.

“We have specific policies around incident response. It consists of guidelines on who is accountable, who is responsible, what notifications need to occur, what actions need to be done” P20_Cons_IR

Interviewees reported that incident response activities are undertaken in a collaborative manner in organisations. Employees with the required skills and knowledge who are mostly individuals with technical skills work together to respond to information security incidents.

“In our organisation incident response is teamwork. We have people who are specialised in detecting incidents, intrusion analysts, malware engineering team, forensics team. So these teams work together with other stakeholders to respond to information security incidents” P21_Cons_IR

“What you normally have, depending on the incidents, is the profiles of the people and the roles that you need. For example, if you need forensic capabilities, you can liaise if you have a forensic team in house. P22_Mng_IR

However, interviewees pointed out that roles and responsibilities for incident response may be undertaken by a formal incident response team in exceptional circumstances:

“I guess I can speak for this organisation which is a very, very large enterprise and due to its size and complexity and the array of businesses around the globe there are multiple teams scattered across the globe who are all tasked with incident response.” P19_Mng_IR

The previous quote indicates that the existence of an information security incident response team depends on the organisation size and availability of resources. In large organisations a dedicated incident response team performs activities such as monitoring, analysing traffic, liaising and coordinating between relevant stakeholders.

Practice 1-Activity 2: Develop incidents classifications criteria
All five interviewees stated that they develop criteria to classify incidents based on their impact on the organisation. This is part of the development of incident response policy and procedures.

“Incident response policy and procedures defines ways to classify incidents, whether it is major or low impact incidents. You’ll have priority or the escalate times or the agreed response times. You have escalation paths. P23_Mng_IR

Several examples of how incidents can be classified according to the impact on the organisation were provided by the participants:
For example, if the impact is only internal to a department or if the impact is widespread in an organisation it would be a different escalation path. Or, if the impact is growing to customers or clients, it would be different.” P22_Mng_IR

The classifications of the incident are important to determine the procedures and resources that are require to handle the incident.

**Practice 1-Activity 3: Schedule incident response training for relevant stakeholders**

Stakeholders (IT and security team members) are experts in their domain so they have the required skills to respond to security incidents. However, all interviewees indicated that there should be training on the organisation’s incident response procedures to increase the readiness of the organisation.

“When you are faced with an incident that has the potential to be major, you need to have the procedures very clear and very rehearsed, and the people need to be well trained on their roles and responsibilities, and how everybody fits in that team.” P22_Mng_IR

“You need to have a good process and train your people. Otherwise, if things strike, you don't know how to react.” P19_Mng_IR

All the interviewees reported that training sessions are conducted in their organisations for employees who may take part in the information security incident response process. These sessions are usually presented as scenario based to assess the readiness of employees and getting everybody aligned with what the procedure says and how to react to an incident.

“assessing the readiness. It is a big part of having standard procedures, documented procedures, and getting everybody aligned with what the procedure says and how to react to an incident. Because, when things happen, it is very difficult to think on your feet” P21_Cons_IR

The role and responsibilities of stakeholders in regard to the incident response process is considered one of the inputs to determine the organisation’s needs for information security and training which is part of the management of ISTA. For more details, see Chapter 7.

**ISIR-Practice 2: Create communication plan**

It was generally agreed amongst the five interviewees that effective communication during an incident plays a significant role in responding to the incident. This practice was also mentioned by twelve participants during the discussion on other ISMPs areas. Participants argued that developing a communication plan is a very important part of the planning and preparation for security incidents.
The ‘Develop communication plan’ practice consists of two key activities: (1) Identify relevant stakeholders and (2) Develop incident information sharing guidelines. Evidence that supports these two activities is presented in the following subsections.

**Practice 2-Activity 1: Identify relevant stakeholders**

All Interviewees reported that they identify relevant stakeholders who should be contacted during incidents. Therefore, interviewees indicated that before the incident occurs, a list of key stakeholders and their contacts should be maintained and kept handy so when an incident happens, it will be easy to contact them for a quick response.

“I think you need to identify your stakeholders beforehand, certainly. You don’t have to go into much detail. It’s very useful to identify the senior stakeholders of the different areas. I’ll say that certainly, the executives, divisional managers, and the business managers are important to get the list.” P22_Mng_IR

Relevant stakeholders include employees with technical capabilities to deal with an incident as well as managers, people who are affected by the incident, are law enforcement. Stakeholders could be internal, that is, employees with the organisation and/or external clients, consultant companies and media.

**Practice 2-Activity 2: Develop incident information sharing guidelines**

As part of the ‘develop communication plan’ practice, all interviewees reported that they develop guidelines for information sharing during an incident. This activity entails defining when and how relevant stakeholders should be notified about an incident, and what information should be shared. The guidelines should specify what means of communication (i.e. email, phone, text, specific tool or software) should be used.

“We have a predefined protocol for communication, like how we will communicate if there is an incident [...] This is the predefined” P21_Cons_IR

It is highly important to share the right information with the appropriate stakeholders. For instance, special software or a communication portal is used in some organisations to communicate with people who are involved in incident response and monitoring, and to keep a record of an incident, who is responsible, what actions have been taken, and what needs to be done.

“So everything is through our communication system. It called Link from Microsoft so we are in touch with relevant stakeholders directly. They can see us online and we can see them so we can talk to each other and we can raise the incident through the system so there is a direct communication.” P20_Cons_IR
It is recommended by the experts that there should be someone who coordinates and liaises between different stakeholders during an incident. He/she should be a “single point of contact”.

“The other important thing is that it needs to be one single point of contact. When you are communicating with a business from an IT perspective, it's important to nominate someone to be that point of contact so there are not different messages, so, coordinating that by a single point. Communication is important.” P23_Mng_IR

8.4.2 The Implementation and Maintenance Stage

This section presents data relating to practices undertaken to respond to incidents. This stage consists of two key practices: (1) Respond to security incidents, and (2) Facilitate lesson learnt from incident. Both practices encompass several activities.

ISIR-Practice 3: Facilitate incident response

All interviewees stated that security manager plays a central and essential role in facilitating, liaising, and coordinating the communication plan and the incident response policy and procedures. This includes conducting an initial investigation, contacting relevant stakeholders, establishing the team, and managing the response activities.

All Interviewees reported four main key activities as part of the ‘Facilitate incident response activities’ practice: (1) conduct initial investigation of the incident, (2) contact relevant stakeholders (Reporting and Notification), (3) establish incident response team, and (4) coordinate and manage the incident response activities.

Practice 3-Activity 1: Conduct initial investigation of the incident

This activity involves conducting an initial investigation of a security event to determine whether it is an incident. Once an incident is detected, it will be appropriately investigated in order to determine what happened, how it happened, and what the impact is. Then it is assigned a priority or severity category according to classification specified on the ISIR policy.

“And you get involved in it because the business needs to understand what's happened, why it has happened, is it a concern and if it is what's the damage or the loss that we might potentially incur. That all needs to be reported up to executive management. What are we doing to fix the problem? What's the financial, reputational implications? What notifications need to be made to external third parties; whether they be vendors, customers, regulators, etc. And making sure that we've closed the gap, validated that the remediation piece works and that this event's not likely to occur again” P19_Mng_IR
Practice 3-Activity 2: Contact relevant stakeholders
At this stage, both the organisation’s incident policy and procedures and the communication plan will be implemented (put into action). Stakeholders must be communicated with, including those who should be involved in responding to the incident and those who are affected by the incident. In addition, management should be briefed about the incident. The level of notification depends on the severity of the incident and its impact on the business.

“And at the same time there might be another team that we speak to around communications and speaking to our customers – in the event of a phishing site that been put up to drive our customers to collect their personal, identifiable information; account information and so forth. We need to obviously contact them. So we’ll have a team that we engage to do that to manage our customers and to understand whose accounts have been compromised.” P22_Mng_IR

“If users detected something unusual, who should be notified, these are the phone numbers they should call and email addresses they need to contact.” P21_Cons_IR

Practice 3-Activity 3: Activate incident response team
Once an incident investigation is conducted, interviewees stated that the organisation should identify and contact personnel who should be part of an incident response team to deal with the incident. The main focus of this identification is to understand the incident in order to find employees with the right skills and knowledge (technical capabilities) to be involved in responding to the incident.

“Well, if you need to scramble a team for that major incident, you need to include that in there. What kind of skills and capabilities do you need? If you need somebody from the technical side, somebody from the network side, someone from the managerial side, somebody to keep in touch with the clients, and somebody to notify the business, too, and have that communication” P22_Mng_IR

The team will be formulated from relevant stakeholders based on the nature of the incident and the roles and responsibilities of the stakeholders. P19_Mng_IR, P20_Cons_IR and P23_Mng_IR, provided in-depth descriptions of how stakeholders are identified and gave several examples of how they would identify stakeholders based on their responsibilities. For example, E5 explained that:

“...there might be a domain team that we need to utilise with anything that's to do with say a fishing campaign. For example, where we need to get the domain taken down. So there will be a team that we identify that we go to engage them to undertake those activities.” P23_Mng_IR
**Practice 3-Activity 4: Coordinate the incident response activities**

Interviewees indicated that once an incident is investigated, the incident response lifecycle will be applied, which include ‘contain’, ‘eradicate’ and ‘recover’ from security incidents. Participants also provided general descriptions of these three activities.

“Then we perhaps look at isolating or containing the threat. In most cases that involves network segregation. So typically, if it's an end point, we just disconnect them from the network and isolate” P19_Mng_IR

“Once you contain, you then go to understand a bit more about the incident and the causes, and how to treat. You start treating the incident and treating first of all the symptoms, because normally the root causes are very, very difficult to treat straight away. You start treating the symptoms, you start getting a plan together; how to scramble a team, what kind of capabilities you need, how do you recover from that? So, I say that the focus is to recover from the incident.” P22_Mng_IR

“If it has a business impact, you need to recover from the incident first and then tackle the root causes later on. The root cause can always wait, but if it is something that the business is suffering from, you need to see how you recover. P22_Mng_IR

The descriptions were mainly technical. The participants reported that incident response lifecycle activities are undertaken by the ISIRT and managed by the security manager or any member of the organisation’s security team.

**ISIR-Practice 4: Facilitate lessons learnt from incident**

The second practice within the implementation and maintenance stage is ‘facilitate lessons learnt from incident’, which involves (1) Debrief relevant stakeholders, and (2) Develop report about the incident. This practice was supported by all five participants and from the remaining twenty-nine, twenty-one participants mentioned this practice.

**Practice 4-Activity 1: Debrief relevant stakeholders**

This activity includes conducting meetings with stakeholders who were involved in responding to the incident to review and discuss activities undertaken to respond to a security incident as well as understand the impact and the cause of the incident.

“And then of course it's undertaking sort of a post-incident review with people that are part of what took place to understand how it happened? What have we done since to prevent it from recurrences? what have we identified that occurred? How do we know it is what we believe it to be? How do we know that we've understood the extent of the threat? So we captured all the possible ways in which this particular threat has entered their environment? How is it propagated within our environment? Have we identified all those potential targets and have they all been
adequately remediated? And then of course what have we done; what patching or what activity have we done to make that no longer a threat.” P19_Mng_IR

The meeting may also result in recommendations such as updating security policy, changing technical controls configurations, and providing an awareness and training program.

**Practice 4-Activity 2: Develop report about the incident.**

It was reported by all interviewees that a report encompassing a summary of the incident information and the recommendations from the post incident review is developed and shared with the stakeholders.

“When there is an incident, we generate an incident report. That incident report actually is generated by one of the managers who usually is not heavily involved in the incident response or incident lifecycle.” P21_Cons_IR

**8.4.3 The Evaluation Stage**

This section discusses practices relating to the review and evaluation of the organisation’s incident response capability and procedures. Most of the review process is performed during the lessons learnt activity of the incident that has been dealt with. This review may include recommendations for changes in the security program, whether they be technological or managerial. One practice was reported as part of this stage: Review of security incident response capability.

**ISIR-Practice 5: Review of security incident response capability**

Thee participants reported that they have annual review of their incident response capability. The review is conducted to check whether the incident response policy and procedures have been followed and determine if the policy needs to be updated. Both internal and external audit could trigger the review of the organisation’s incident response capabilities.

“It’s normally included in internal audits or even external audits, so you can assess your capability against different standards. For example, if you are certified by the 27001 standard, you can have an external auditor that assesses your capability and how you manage incidents as a whole. When the audit comes, and I’ve been in such audits, what you normally do is you have a sample. The auditor comes in or their viewer comes in and you have all the major incidents that happened in six months or a year, depending. They go through the sample and they pick a few incidents and they follow through. They ask to see how the incident was logged so that the record and the software that you used to manage an incident is that--they ask to see the reports and see how you responded to that. Who was part of a team?” P22_Mng_IR
Three activities were reported by the participants as part of the ‘conduct a periodic review of security incident response capability’ practice: (1) Review the incident response policy and procedures, (2) Update the communication plan, and (3) Develop incident response report.

**Practice 5-Activity 1: Review the incident response policy**
As part of periodic review of the ISIR process, the participants stated that the incident response policy and procedures is reviewed.

> “we also always update [IR] policies, procedures and other continuing process. We are continuously updating all the procedures. Our policies are updated either they are updated every six months or they are updated based on external even incident, some incident happened and we found out, okay. Our policy was not covering this, our procedures were not there, so we go ahead and modify and due to an event.” P21_Cons_IR

The experts mentioned that the review of the policy happens after major incidents. The review may be also conducted as part of the annual internal or external audit process.

**Practice 5-Activity 2: Update the communication plan**
All participants emphasised the need for keeping the communication plan up-to-date to ensure effective communication during incidents. They stated that the list of key stakeholders and their contacts should be reviewed and updated. The review and update usually done in a monthly basis.

> “We always make sure that our communication plan is current and up-to-date. So we may add new people, update their role and their emails and phone numbers” P22_Mng_IR

**Practice 5-Activity 3: Develop periodic incident response report**
The participants reported that it is important to develop a periodic report of incidents whether it is quarterly (every three months) or every six months, with all the incidents that occurred during this period, and share it with relevant stakeholders, such as executives and teams within the security department (policy team, ISTA team, and auditors).

> “In my organisation we generate a full incidents reports let say every six months and share it with management and other stakeholders in the organisation” P23_Mng_IR
8.4.4 Summary of the findings

This section discusses changes to the proposed framework of ISIR management practices as a result of the empirical refinement and validation via semi-structured interviews with information security experts. The empirical data has provided rich understanding of the management process of ISIR in organisations which led to many changes in practices and activities in the preliminary framework. The changes range from adding activities, reorganising practices and activities, moving practices from stage to another. Table 8-3 presents the refined framework of ISIR management practices.

Table 8-3 The refined framework of ISRM practices

<table>
<thead>
<tr>
<th>Stage</th>
<th>Practice</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Create incident response policy</td>
<td>Define roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop incident classification criteria</td>
</tr>
<tr>
<td></td>
<td>Create communication plan</td>
<td>Schedule incident response training for relevant stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identify relevant stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop incident information sharing guidelines</td>
</tr>
<tr>
<td>Implement &amp; maintain</td>
<td>Facilitate incident response</td>
<td>Conduct initial investigation of the incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact relevant stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Activate incident response team</td>
</tr>
<tr>
<td>Evaluate</td>
<td>Facilitate lessons learnt from incident.</td>
<td>Debrief relevant stakeholders</td>
</tr>
<tr>
<td></td>
<td>Review security incident response capability</td>
<td>Develop report about the incident.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review the incident response policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Update the communication plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Develop periodic incident response report</td>
</tr>
</tbody>
</table>

In the development stage, in response to the interviewees answers on the practice *Create incident response policy and procedures*, three activities were added in the framework:

The ‘Define roles and responsibilities’ was added because there was wide agreement amongst all interviewees that as part of the development of the incident response policy and procedures, roles and responsibilities are defined. This includes providing general guidelines of the incident response team (structure and responsibilities).

There was strong support for the activity *Develop incident classification criteria* from the experts. All the interviewees emphasised the importance of developing criteria and
classifications that can be used to determine whether the incident should have high, medium or low priority in terms responding efforts. Therefore, there was enough evidence that this is an activity rather that mentioning it as just an element of the incident response policy.

The Schedule incident response training for relevant stakeholders in the organisation who are expected to be involved in responding to incident’ activity was originally placed under the Establish incident response team practice. However, the evidence indicated that this activity should be moved this activity to the Develop incident response policy and procedure practice as a better understanding of the nature of the ISIRT in organisations was developed. See discussion about the change in Establish incident response team practice.

The Develop communication plan and activities under this practice were unchanged. Although two participants indicated that the develop communication plan practice is part of develop incident response policy and procedure practice, three participants asserted that it should be a separate document. They argued that the communication plan is more dynamic and update and changes are done more regularly than the ISIR policy. Therefore, this practice and its activities remain unchanged.

There was no strong evidence that organisations establish the ISIR during the development stage of the ISIR management process. The data showed that incident response is done in a collaborative manner by different stakeholders in the organisations. In practice, organisations identify relevant stakeholders, which include personnel with different skills and capabilities (mostly technical), as part of the ‘develop communication plan’ practice. Then, once an incident occurs, the team is established from the stakeholders based on the incident type and complexity. Therefore, establish incident response team became an activity of the Facilitating incident response activities practice in the implementation and maintenance stage.

Many changes occurred in the implementation maintenance stage, as the data provided more understanding of the managerial level practices. The literature focused on the technical practices performed as part of the incident response lifecycles; the data explained managerial practices undertaken once an incident is reported.

The practice respond to security incident was replaced by the Facilitate incident response practice. As the focus of this study is on the managerial practices, the data showed that a key managerial practice is to Facilitate incident response. This practice includes the following activities:
• Conduct initial investigation of the incident: this activity involves understanding the nature of the incident, its impact, and causes.

• Contact relevant stakeholders: in this activity, reporting and notifying to relevant stakeholders (management, employees, and customers) take place.

• Activate incident response team: this activity entails formulating the incident response team based on the understanding of the incident. Participants reported that the selection of the team members is subject to the type of the incident.

• Coordinate the incident handling activities: In this activity steps and measures are undertaken (mostly technical) to handle the incident.

The Facilitate lesson learnt from incident practice was added. The professional and academic literature included lessons learnt and post-incident review as the last step in the incident response lifecycle. Consistent with the literature, all participants reported that in practice, this lesson learnt and post-review is undertaken after the incident has been dealt with. It was concluded from the participants’ comments that ‘Facilitate lessons learnt from incident’ is a key managerial-level practice that is undertaken by security managers and/or by security personnel who are responsible for managing the ISIRT. Thus, the evidence supported that this practice as a main practice within the implementation and maintenance stage. The Facilitate lessons learnt from incident practice consists of two activities: Debrief relevant stakeholders who were involved in responding to the incident and Develop report about the incident.

In the evaluation stage, although the evidence indicates that organisations conduct a thorough review and evaluation of the ISIR. However, from the discussion with the participants, they reported that a review may take place as part of an external and internal audit. Three activities were supported: review the incident response policy and procedures, update the communication plan, and develop periodic incident response report.

8.5 Final validation
To perform the final validation of the framework an email was sent to each of the five participants to provide feedback on the framework and comments on whether the practices and key activities are comprehensive. Only three participants have responded to the email with their comments and feedback on the framework.
For the first question “Do you think the framework covers key activities done in organisations to manage security incident response?” all three participants answered ‘yes’ and they provided the following comments:

“I think this framework covers at a high level all the relevant stages to be followed by a security incident response management framework and at the same time simple to aid understanding and facilitate its implementation. This framework would prove valuable for companies aiming at implementing and improving their capabilities in this area”. P22_Mng_IR

“This framework is practical and should be adopted by the organisations to manage their incident response process” P20_Cons_IR

A suggestion was provided by P23_Mng_IR that

It would be more valuable if you may include a communication activity after the completion/development of incident report into stage 2. You may include a statement “Develop and Communicate report about the incident” so that all the stakeholders are fully aware and informed about the outcome of the incident.

The incident response report should be shared with the relevant stakeholders (e.g., management, teams of other ISMPs areas). This is important to leverage the experience and lesson learned from responding to security incidents to improve other areas of practice and therefore the overall effectiveness of the organisation information security program.

8.6 Discussion

The analysis of the empirical data enabled a rich understanding of the managerial practices of ISIR undertaken in organisations. The main contribution of this study is the identification of the set of key activities that are required to response to incidents and the extent to which these activities are implemented in organisations. The set of key activities are comprehensive and exhaustive. No other key activities were identified from any of the organisations represented by the participants. The findings have provided an insight of how these key activities have been institutionalized and how well they have been resourced. Following is a discussion of the findings related to ISIR management practices.

8.6.1 Focus on managerial practices rather than technical

Considerable work in the ISIR domain has focused on handling incidents rather than managing the entire process within an organisation. Therefore, aspects such as planning and preparation for incidents and the overall evaluation of the process of security incident response have received little attention in both research and practice.
During the interviews, the participants in this study provided thorough and extensive discussion of the incident response lifecycle and little attention was given to planning and establishing the organisation’s incident response capabilities and conducting periodic review and evaluation of the entire incident response. This finding was consistent with the literature, as much of the research in the area, especially ISIR approaches emphasise the technical perspective of the ISIR process and recommend technological practices (Ahmad, Hadgkiss, et al., 2012; Jaatun et al., 2009; Shedden, Ahmad, et al., 2011).

This limited view of the process is inherited from the view of the information security domain (Ahmad, Hadgkiss, et al., 2012). The focus on the practices undertaken is to handle an incident rather than the overall all management of the ISIR process is one reason behind this limited view of the process. Several researchers argued that technological, human, and organisational factors of the ISIR process should be taken in consideration when developing, implementing, and evaluating the process (Ahmad, Hadgkiss, et al., 2012; Jaatun et al., 2009).

8.6.2 Importance of planning activities for the ISIR process

Participants considered the overall establishment of the information security program (identifying and managing risks, establishing ISP, developing the ISTA program and implementing technological controls) as the planning and preparation of the ISIR process. This is similar to the view of incident response guidelines (ENISA, 2010a; Northcutt, 2003). While it is true that the aim of establishing an information security program is to protect the organisation’s information resources, it is not possible to prevent all incidents, given the circumstances and interconnectivities in this day and age. Therefore, proper procedures and plans must be in place to respond to incidents once they occur.

There is wide agreement in the literature that planning is an important element of the incident response process. Researchers stressed that effective incident response depends on having a well-documented incident response plan (Jaatun et al., 2009; Line et al., 2014; Tan et al., 2003; Tøndel et al., 2014). However, several studies (Line et al., 2014; Tan et al., 2003) concluded that there are inadequate planning and preparation activities undertaken (i.e. well-developed and rehearsed security incident response policy and procedures) by organisations. The findings of this study indicate that organisations are well-aware of the importance of planning and preparation for security incidents. Several practices are implemented, such as create incident response policy and procedures, create communication plan. Further, the evidence suggests that substantial effort and resources are placed on technologies to analyse network traffic and detect
incidents. There was no strong evidence that indicates that organisations have established a formal planning and preparation practices for incident response. This is, of course, subject to the level of maturity and availability of resources in the organisation. This research argues that there are several reasons for the lack of focus on planning activities. First, organisations do not have sufficient guidance on planning and preparing for incident. Second, the technological view of the process also contributes to the lack of planning activities for incident response. Third, the dynamic nature and the increase in the number and consequences of security incidents make it very challenging to follow one procedure so the focus is just to detect and respond rather than develop policy and procedures that might serve as general guidance, not to be followed step-by-step as the participants indicated.

**8.6.3 Incidents related to the human aspect**

Several participants emphasised the increase in the number of incidents in their organisations. Participants also reported that incidents caused by the organisation’s employees constituted a large proportion of the overall number of those incidents. They provided examples of incidents happened that because employees shared their passwords, clicked on links sent by phishing emails, and sent confidential documents to their personal email. Participants argued that the development of an ISTA program is important for overcoming incidents related to human behaviour and noncompliance with security policy. This finding is in accordance with the literature where several studies (Öğütçü et al., 2016; Tsohou et al., 2015) regarded humans as ‘the weakest link in the security chain’ and recommended the establishment of a ISTA program. See Chapter 7 for more details on ISTA.

**8.6.4 ISIRT: structure and communication**

There is a consensus in the literature on the importance of establishing an ISIRT (Hove et al., 2014; Michael, 2002; Northcutt, 2003). Several issues related to ISIRT are discussed in the literature. These issues include the structure and the size of the team, roles and responsibilities, required skills and knowledge and communication and collaboration between relevant stakeholders and the team (McLaughlin et al., 2017; Steinke et al., 2015; Sundaramurthy et al., 2014).

In terms of the structure of the incident response team, the participants of this study reported that there is no standing team (formal/dedicated) for incident response in their organisations. It is a collaborative exercise undertaken by the relevant personnel within the security and IT
department depending on the nature of the incident. As explained on Section 8.4.1, the organisations maintain an up-to-date list of relevant stakeholders and their contacts and once an incident is detected and thoroughly investigated the personnel with the appropriate skills and knowledge are identified and contacted. The process of establishing an ISIRT as reported by the participants is similar to the description of incident response team reported by AS/NZS ISO 18044 “Within most organisation the ISIRT will be virtual team, with a senior leading the team supported by groups of individuals specialised in particular topic, e.g. in handling the malicious code attacks, who will be called upon depending on the type of incident concerned” (pp4 AS/NZS ISO 18044).

The success of this type of structure depends on the communication and cooperation between stakeholders. This is very important when team members are working in different locations (i.e., different branched of an organisation and/or customer sites)

Therefore, one of the key practices reported by the participants is the ‘develop communication plan’ practice as a key practice in the development stage. This practice involves identifying stakeholders and developing guidelines for communication. To ensure effective communication, participants recommends the implementation of special software to communicate with relevant stakeholders and keep them informed about incident status. Participants also recommended that to ensure effective communication, it is important to delegate coordinating and liaison duties between different stakeholders during an incident to a member within the team, usually the leader of the incident response team who works as a “single point of contact”.

### 8.6.5 Review and evaluation of incident response

The findings of this study revealed that the evaluation and review of the organisations tended to adopt a narrow technological evaluation and focus on high impact incidents. Although some activities were identified by the participant as part of the overall of the organisation’s incident response capability, these activities are usually conducted as part of the audit process.

One of the key issues regarding incident response review is around the scope of the learning from an incident. Most of the research talks about learning from a technological point of view not from a strategic management point view. Several studies have focused on learning from security incidents. They point out the importance of review and learning from experience and knowledge accumulated from responding to a security incident to improve the overall
information security management (Ahmad, Maynard, et al., 2015; Tøndel et al., 2014). (Shedden, Ahmad, et al., 2010, 2011) stated that learning from incidents in organisations was informal and adopted a single loop approach where experience and knowledge gained from responding to incidents are used to review policy, update risk assessment (adding risks, changing the rate of existing risks). However, double loop learning which questions the process that led to an inaccurate risk assessment, insufficient, misleading or contradictory advice in policies, ineffective or misaligned strategies, and inadequate security training and awareness (ISTA) was not adopted in organisations. The study findings uncover that, in practice, despite the literature pointing out that double loop learning is important to improve information security program, there was no evidence of the double loop learning.

8.7 Summary
This chapter presented the development, and refinement of the ISIR management practices framework. It started by providing an overview of the literature in information security incident response, highlighting gaps and deficiencies related to the incident response process. Then a framework was developed based on a rigorous and systematic review of the literature. The refinement and validation of the proposed framework was also presented. The chapter ended with discussion of the findings from the empirical data. The next chapter will present the development of the information security intra organisational liaison management framework.
Chapter 9 INFORMATION SECURITY INTRA-ORGANISATIONAL LIAISON MANAGEMENT PRACTICES

9.1 Introduction
The findings presented in previous chapters (5-8) indicated that there are several key practices and activities within ISMP areas that depend heavily on the participation and involvement of various stakeholders within the organisation. The success of these practices relies on how effective security personnel communicate with those stakeholders to engage them in undertaking those practices.

However, the review of the literature uncovered that although there is broad consensus in the literature on the importance of stakeholder involvement in the security management process, there is a lack of guidance on the practices that should be undertaken by security managers to effectively communicate, involve and engage stakeholders in the process. Therefore, it seems to be an area of practice that is assumed to occur with little systematic guidelines.

One of the key findings of this research project, is the identification of practices undertaken by security managers to communicate effectively with stakeholders in the ISM process. The identification of such practices addresses the gap in the literature by providing guidance to organisations and enabling ISMPs.

This chapter is organised as follows. Section 9.2 reviews the literature that focus on the role of stakeholders on the ISM process and the importance of effective communication, highlighting gaps and deficiencies. Section 9.3 discusses the need for IOL management practices and draws from organisational communication literature. Section 9.4 presents the analysis process of empirical data which leads to the identification of information security IOL management practices. Section 9.5 discusses the contribution and implications of the findings and how they
fit with the comprehensive ISMPs framework. Section 9.6 provides a summary of the chapter and introduces the next chapter.

9.2 Literature Review
This section presents the literature on two closely related concepts: stakeholder involvement in the ISM process and communication between stakeholders and the information security team. These concepts enable better protection of the organisation’s information assets through the integration of ISMPs into the business process.

9.2.1 Stakeholders’ involvement in the information security management process
Several researchers argue that to manage information security effectively, stakeholders need to be involved in the process, because information security is a multidisciplinary issue that requires the involvement of multiple stakeholders with a wide variety of skills from different departments within the organisation (Kandogan & Haber, 2005; von Solms, 2001; Wood, 2004). In this study, the term stakeholders refers to “organisational members from the functional areas of business, from non-managers through the ranks of senior management” (Spears & Barki, 2010, p.507).

The benefit of stakeholders’ involvement in ISMPs
Through the participation of stakeholders in the development, implementation and evaluation of ISMPs, stakeholders can attain considerable awareness of the risks, and the policies and procedures that are in place to mitigate those risks (Tøndel et al., 2014). This awareness can positively influence stakeholders’ behaviour and attitude towards information security and subsequently, their compliance and adherence to organisational information security policies and procedures (Furnell & Rajendran, 2012; Safa et al., 2015). Low levels of involvement can result in a decreased awareness, negatively influencing employees’ information security attitudes (Flores, Antonsen, & Ekstedt, 2014).

Further, stakeholders’ involvement in ISMPs can also lead to better alignment between ISMPs and business objectives. This improved alignment is because the involvement of stakeholders provides the necessary business knowledge and understanding of the specific organisational context that is required to achieve alignment with business, thus contributing to more effective ISMPs (Spears & Barki, 2010). In the same vein, Flechais and Sasse (2009) argue that “the
biggest benefit of involving stakeholders in the security process was that it was possible to directly elicit their point of view. This provided very rich information about security needs, constraints and limitations that would be acceptable to the different stakeholders.” (P.292). In other words, stakeholders’ involvement ensures that their views and feedback on the ISM process are considered during the application of ISMPs.

The level and the nature of stakeholders’ involvement in ISMPs
Information security management practices (ISMPs) are undertaken in organisations within various areas of ISM, including risk management, policy management, and incident response management, as well as information security training and awareness. Their successful integration into the organisation more broadly as mainstream practices depends heavily on the contributions of other individuals and resources (Singh, Picot, Kranz, Gupta, & Ojha, 2013). Stakeholder involvement is very important for effective implementation of ISMPs and, ultimately, the protection of organisational information assets. The review process of the information security management literature shows that the general view supports the importance of stakeholders’ involvement in the information security management process (Ruefle et al., 2014; Tøndel et al., 2014). The literature also endorses the argument that management practices cannot be undertaken in isolation from other departments (Safa et al., 2015; Wood, 2004). Table 9-1 summarizes the nature of stakeholder involvement in ISMPs.

9.2.1 Communication between the information security team and internal stakeholders
The involvement of the entire organisation in the information security process requires communication, collaboration and cooperation among stakeholders at many levels in the organisation. ISM literature highlights the importance of effective communication in achieving high levels of stakeholder involvement (Björck, 2005). Effective communication is one of the most cited factors for the success of the ISM process (Kraemer et al., 2009).

As highlighted in the previous section, each ISMP area contains many practices that rely on the participation and involvement of multiple stakeholders. To achieve high levels of involvement, the security team in an organisation needs to communicate with relevant stakeholders and motivate them to participate, share their knowledge, comply with policy, report incidents and assist in the risk management process. Werlinger, Hawkey, Botta, and Beznosov (2009) conducted a study to investigate the context of interaction between information security practitioners and other stakeholders in the organisations. They identified nine activities that
require communication between the organisation’s security team and other stakeholders. These activities are: perform and respond to security audits, design services incorporating security requirements, solve IT security issues of end-users, implement security controls, mitigate vulnerabilities, administer security devices, respond to security incidents and develop security policies (Werlinger et al., 2009). The analysis of the literature found that there is a need for effective communication when conducting ISMPs.

**Table 9-1 Summary of stakeholders’ involvement in ISMPs from the literature**

<table>
<thead>
<tr>
<th>ISMP area</th>
<th>Summary of stakeholders’ involvement</th>
<th>Representative references</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy management</td>
<td>The literature highlights the importance of involving multiple stakeholders in security policy development and its impact on the quality of the policy, compliance and user acceptance. Stakeholders should be part of the policy development team. They should also provide feedback on the policy and play a major role in enforcing the policy.</td>
<td>Doherty and Fulford (2006); Kadam (2007); Maynard and Ruighaver (2003); Maynard et al. (2011); Rees et al. (2003); Siponen et al. (2014)</td>
</tr>
<tr>
<td>ISTA management</td>
<td>Stakeholders provide feedback and input to ISTA practices, including identifying ISTA program requirements, establishing the ISTA team, developing the ISTA materials, and implementing and evaluating the program.</td>
<td>Kim (2014); Tsohou et al. (2015); Wright (2005)</td>
</tr>
<tr>
<td>Information security risk</td>
<td>The involvement of users provides needed business process knowledge, resulting in greater alignment between information security risk management and the business environment. Alignment will improve security risk management and enabling the organisation to implement effective risk mitigation security controls.</td>
<td>AS/NZS ISO 31000:2009; Bernard (2007); Spears (2006); Spears and Barki (2010)</td>
</tr>
<tr>
<td>Incident response management</td>
<td>Preventing and minimizing the impact of security incidents requires variety of skills and knowledge. Therefore, incident management can involve various part of an organisation.</td>
<td>Ahmad, Hadgkiss, et al. (2012); Ruefle et al. (2014); Tøndel et al. (2014)</td>
</tr>
</tbody>
</table>

**Policy and Communication:** - In the policy management area, establishing the policy development team and reviewing and approving security policy requires a great deal of communication, consultation and collaboration between team members and other stakeholders, including managers and members of other departments. Successful communication of policy leads to better compliance with policy by employees (Werlinger et al., 2009). Therefore, if the policy is well communicated, the enforcement of the policy will be a much easier task. Communicating the policy assists the organisation to manage change in its processes as a result of the implementation of new policy (Maynard & Ruighaver, 2003). Communicating the policy has three main objectives: to make users aware of the policy, to explain the reason for
implementing the policy, and to demonstrate how it will affect them and what the implications are if they do not comply with it (Kenneth J. Knapp et al., 2009; Maynard & Ruighaver, 2003).

**ISTA and Communication:** - Communication is also important for several practices within ISTA management. Organisations need to communicate with stakeholders in order to motivate employees to participate in the program. This is done by explaining to management and employees how participation in the ISTA program will benefit the organisation (Wilson & Hash, 2003). Further, as implementing ISTA involves conducting training sessions, seminars and briefings, effective implementation requires effective communication. Evaluating the effectiveness of ISTA includes communicating with participants in the program to encourage them to provide feedback, and suggestions on how to improve the program. Wright (2005) states “security managers need to liaise with other employees to obtain their feedback on the material, presentation and the level of awareness and training within the organisation” (p.11).

**Risk Management and Communication:** - In the information security risk management area, risk assessment, which is the core of the risk management process, entails ongoing communication and information sharing between the information security management team and key organisational stakeholders (Spears & Barki, 2010). This includes all members inside the organisation, such as managers and employees from different departments (Whitman & Mattord, 2008).

**Incident Response and Communication:** - Communication is very important in security incident response management (Ahmad, Hadgkiss, et al., 2012; Steinke et al., 2015). Reporting security events and communication with different stakeholders during a security incident is an essential part of the incident response management process (Steinke et al., 2015). The success of an information security incident response process lies in effective communication, as it has an instrumental effect on the effort to respond to incidents, while communication breakdown can undermine the entire incident response process (Björck, 2005; Kraemer et al., 2009). According to Ahmad, Maynard, et al. (2015), the process of learning from experiences gained from responding to past incidents to improve other areas of ISM, such as risk management, policy management and ISTA management, requires effective communication between the organisation’s incident response function and information security function, and that the lack of communication and cooperation between those two functions may suggest that organisations are not learning from their incident experiences.
Communication with stakeholders, each with different backgrounds and at different levels, is a very complex and challenging task for information security personnel (Werlinger et al., 2009). The organisation’s security team has to be fully aware of the context and strategies of communication with stakeholders. Therefore, this paper argues that together, the communication strategies that security personnel need to engage in with the rest of the organisation can be termed “intra-organisational liaison management”. This research defines intra-organisational liaison (IOL) management practices as a set of activities undertaken by information security personnel to communicate effectively with internal stakeholders and, therefore, increase their participation and involvement in the information security management process. The “intra-organisation liaison” term has been used in industry standards such as NIST (Swanson & Guttman, 1996) in a similar vein.

While the literature identifies that security management requires collaboration among stakeholders, there is a lack of guidance on how security managers interact and communicate with other stakeholders within the organisation. (Kandogan & Haber, 2005; Werlinger et al., 2009). Therefore, there is a gap in the literature about how security personnel should be communicating with other parts of the organisation more strategically and effectively. Communication is often mentioned without clear guidelines and planning. Hence, this paper proposes a model which offers guidelines for security personnel in the area of inter-organisational liaison.

9.3 Towards a Model of Intra-Organisational Liaison Management Practice

Undertaking IOL practices is more than an incidental and operational day-to-day activity. It needs to be recognized as a practice that should be articulated, strategized and planned for.

Researchers contend that security managers are responsible for liaising and coordinating between stakeholders involved in the ISM process. For example, Werlinger et al. (2009) suggest that organisations should establish strategies for communicating security issues to stakeholders that will assist them to be proactive in continually establishing mutual understanding so that they can build a common ground for joint activities. Moreover, Puhakainen and Siponen (2010) called for institutionalization of communication-related activities.

The role of intra-organisational liaison management can be articulated in three words: communication, collaboration and coordination (Savola et al., 2006). It involves two-way
communication between security managers and the rest of the organisation. Having two-way communication will ensure security managers are able to stress the importance of security in achieving organisational goals (Purser, 2004a) and allows stakeholders to ensure that organisational procedures are defined with respect to security (Tu & Yuan, 2014). To develop IOL guidelines for information security personnel, this thesis draw on both the ISM literature and the organisational communication literature to identify key areas for practice and further research.

**9.3.1 Internal communication in the organisational communication literature**

The concept of internal communication has been widely discussed in the organisational communication literature. There is substantial literature that suggests that internal communication has a significant effect on the success of organisations (Welch & Jackson, 2007). Researchers argue that the engagement of stakeholders requires clear, consistent and continuous communication (Saks, 2006). Welch and Jackson (2007) assert that internal communication is vital for the success of organisations as it enables strategic managers to engage employees and achieve objectives. Effective internal communication improves relationships with stakeholders resulting in increasing employee commitment, promoting a positive sense of belonging in employees, developing their awareness of environmental change, and developing their understanding of the need for the organisation to evolve its aims in response to, or in anticipation of, environmental change (Welch & Jackson, 2007).

There are four main elements involved in the communication process in organisations: the sender, the receiver, the message and the medium being used to deliver the message (Lawrie, Shulver, & Antarkar, 2015) Successful communication requires that the sender sends a clear message using an appropriate medium to ensure that the receiver understands the message. This also requires enabling the receiver to respond to the sender to provide feedback and input. It is a two-way communication channel. According to Ellyard, Koritschoner, and Braham (2002), communication breakdown can happen if the message does not reach the receiver or the receiver misunderstands the message.

The literature also highlights the importance of ensuring that an organisation’s members have the necessary skills, such as knowing how to give and receive feedback and how to negotiate and solve any conflicts that may result from communication (Ellyard et al., 2002). Therefore, it is suggested that organisations provide a training program for their employees.
Management literature also discusses aspects of internal communication. These aspects include
the participants, the direction and the content of the communication (Welch & Jackson, 2007).
In terms of participants, Freeman (2010) identified a range of internal stakeholders, including
line management (boss and boss’s boss), team members, and other internal groups (related
departments, subsidiary managers). The information on direction of internal communication has
also discussed several types of communication flow between participants. These include one-
way or asymmetrical, vertical or downward, lateral or horizontal, and upward communication.
Welch and Jackson (2007) developed an internal communication matrix (shown below in Table
9-2). They stated that the matrix can be used by academics and professionals to analyse internal
communication, which can assist in evaluating internal communication and developing
effective strategies.

**Table 9-2 Internal communication Matrix adopted from (Welch & Jackson, 2007)**

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Level</th>
<th>Direction</th>
<th>Participants</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal line management communication</td>
<td>Line managers/ supervisors</td>
<td>Predominantly two-way</td>
<td>Line managers-employees</td>
<td>Employees’ personal impact, e.g. appraisal discussions, team briefings</td>
</tr>
<tr>
<td>Internal team peer communication</td>
<td>Team colleagues</td>
<td>Two-way</td>
<td>Employee-employee</td>
<td>Team information, e.g. team task discussions</td>
</tr>
<tr>
<td>Internal project peer communication</td>
<td>Project group colleagues</td>
<td>Two-way</td>
<td>Employee-employee</td>
<td>Project information, e.g. project issues</td>
</tr>
<tr>
<td>Internal corporate communication</td>
<td>Strategic managers/top management</td>
<td>Predominantly one-way</td>
<td>Strategic managers-all employees</td>
<td>Organisational/corporate issues, e.g. goals, objectives, new developments, activities and achievements</td>
</tr>
</tbody>
</table>

Understanding aspects of internal communication and adapting them to the context of
information security can be of great benefit in addressing the needs for clearer guidelines and
strategic planning for the communication process between information security personnel and
internal stakeholders, and for embedding the communication process into mainstream
information security as part of resourcing for implementing information security policies and
practices.
9.3.2 Recommendations for effective communication and stakeholders’ involvement in ISM literature

The review of ISM literature uncovered recommendations and suggestions for information security personnel to communicate better with stakeholders. These suggestions include, establishing good relationships with stakeholders and assigning clear roles and responsibilities with regard to security practices. Flechais and Sasse (2009) highlight the importance of involving all stakeholders in information security suggesting that to motivate stakeholders to participate in the security process and take their share of the responsibility, the organisation should assign responsibility, make security requirements explicit and provide clear communication about security between stakeholders. Similarly, Puhakainen and Siponen (2010) recommend that organisations 1) integrate training and information security communication into normal business communication, 2) develop a process to make information security communication a continuous activity in the organisation, and 3) involve management, security staff and users in the communication process.

The involvement of stakeholders can also be improved by developing good relationships with stakeholders. According to Markus and Mao (2004) and Taylor et al. (2013), developing good relationships with stakeholders is likely to result in a high level of participation in the ISM process; bad relationships, on the other hand, tend to yield bad outcomes. Good relationships enable the security team to understand stakeholders’ needs and ensure they understand the purpose of their involvement. It also prevents disagreements that occur during the process that result in hindering stakeholders from participating in the ISM process (Markus & Mao, 2004; Taylor et al., 2013).

One of the important recommendations for improving stakeholders’ involvement in the ISM process is to gain the support of top management. Researchers (e.g., Kenneth J Knapp, Marshall, Rainer, & Ford, 2006) have stressed the importance of top management support and involvement in the security management process. Business executives play a vital role in providing a strategic view, which is crucial for aligning information security requirements to the business objectives of the organisation (Singh et al., 2013). Top management are responsible for ensuring that adequate resources are allocated to the ISM process in order to achieve the organisational business objectives (Hu et al., 2012). Therefore, gaining the support of this important stakeholder can have a significant influence on the involvement of other types of stakeholders (Kankanhalli, Teo, Tan, & Wei, 2003).
9.3.3 Why InfoSec IOL differs from general IOL/ org communication

In Section 9.2, it was explained that the success of the information security management process depends on the participation and involvement of various stakeholders in the organisation, and that effective communication is vital for involving stakeholders in the process. This section explains why communication regarding information security differs from other internal communication in organisations and why recommendations and suggestions for effective communication in general need to be adapted to suit the specific context of information security.

Information security communication differs from other organisational communications for several reasons. First, there is a commonly held yet mistaken belief that security controls do not require involvement of stakeholders outside the security department. Successful implementation of information security controls requires the involvement of all stakeholders to ensure they understand the need for such controls and their intent which ultimately results in relatively higher level of end-user acceptance.

Second, information security personnel responsible for communicating with stakeholders usually have developed strong technical skills but have not been trained to communicate with non-security personnel. They may need additional support and resources to communicate effectively and to provide and receive feedback with stakeholders (e.g. without the use of technical jargon).

Third, in many organisations non-security personnel have low security awareness including low appreciation for security threats and the associated impacts. Unlike in the case of information technology (IT), where IT artefacts are developed and used by stakeholders, information security is less visible to stakeholders. Low levels of security awareness and lack of appreciation for security risk ultimately makes it more challenging to communicate messages related to information security.

Last, certain types of communication in information security are uniquely constrained by laws and regulations (e.g. privacy regulations, competition laws, confidentiality contracts). Further, in certain circumstances where the organisation is experiencing a major incident, security personnel must communicate with stakeholders in a high-pressure environment where information load, information diversity and degree of uncertainty is high, and the structure of the environment is changing rapidly and continuously.

The complexity of the area, the nature of the communication and the people involved in the process provide motivation to address the need for clear and sufficient guidance for information security.
security personnel on how to communicate effectively with stakeholders and, therefore, increase their participation in the process of information security management.

9.4 Data analysis and Findings
As mentioned in Section 3.5.1, thirty-four interviews were conducted with security experts from different type of organisations. In each interview, participants were asked to discuss one of the ISMPs areas (policy management, risk management, ISTA management and incident response management) (see Section 3.5.1.1 for more details on the interview protocols). During the discussion about the managerial activities undertaken by organisations within a specific area of ISMPs, the participants reported several activities that require the participation of various stakeholders within the organisation. Therefore, the researcher had initially included questions about:

1. The identification of stakeholders
2. Type of stakeholders and their role in the process
3. Methods and tools used to communicate with stakeholders
4. The best strategies to communicate with stakeholders and encourage them to participate in the process
5. Ways to measure the effectiveness of communicate with stakeholders

All thirty-four interviews were transcribed which resulted in approximately 250 pages of transcribed text. All data related to the questions 1-5 above was combined in one document. It consists of 30 pages of transcribed text. Then the data was coded sentence-by-sentence to identify the practices (themes) and activities (subthemes) undertaken by organisations as part of IOL management.

As described in Section 3.6, the data was coded using thematic analysis technique (Boyatzis, 1998; Lee et al., 1999) and grounded theory analysis approach (Strauss & Corbin, 1998). The results of the coding process resulted in the identification of IOL management practices depicted in Table 9-3.

Table 9-3 presents IOL management practices into the three institutionalisation stages: the development, the implementation and maintenance stage, and the evaluation stage. There are two key reasons to classify the identified IOL management practices in these three stages. First, to follow the same classification pattern of other ISMP areas as the literature suggest that practices within those areas are usually presented in phases and stages. Second, the nature of
the identified practices supports the decision to group them into the suggested stages. For example, the identification and the development of the communication protocol are development practices while performing the communication is implementation. Further, validating and measuring the effectiveness of the communication process is an evaluation practice.

**Table 9-3 information security IOL management Practices**

<table>
<thead>
<tr>
<th>Stage</th>
<th>Practice</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop</td>
<td>Identify relevant stakeholders for information security</td>
<td>Determine the context and the level of involvement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Establish a good relationship with internal stakeholders.</td>
</tr>
<tr>
<td></td>
<td>Develop communication protocol</td>
<td>Assign security personnel for communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map the appropriate method of communication with stakeholders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schedule training on communication skills for security personnel</td>
</tr>
<tr>
<td>Implement &amp; Maintain</td>
<td>Facilitate communications with stakeholders</td>
<td>Providing feedback and security reporting to other functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Soliciting stakeholders’ feedback</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prioritising and consolidating stakeholders’ views in light of business needs</td>
</tr>
<tr>
<td>Evaluate</td>
<td>Review the effectiveness of communications between other part of the organisation and the security team</td>
<td>Identify indicative success metrics of how well security issues are communicated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Measure the level of engagement of employees in security practices</td>
</tr>
</tbody>
</table>

The following sections present IOL practices identified in the coding process which the organisation undertakes to enable ISMPs of other.

### 9.4.1 The development stage

In the development stage of IOL management practices, the interviewees reported two key practices security teams undertake to liaise with internal stakeholders. These practices are: (1) Identify relevant stakeholders and (2) Develop communication protocol. Each practice consists of several activities. The following sections discuss these practices and its activities.

**IOL-Practice1: Identify relevant stakeholders for information security**

In each of the interviews conducted participants reported that identifying relevant stakeholders for each information security management area, is an important practice. All thirty-four interviewees stated that relevant stakeholders play a key role in the security management process. Therefore, stakeholders should be identified to involve, and engage them in the process.
One important stakeholder, mentioned by nearly all interviewees across all ISMP areas, is top management. The interviewees contend that leadership involvement and understanding of security problems is important to encourage other stakeholders (middle management and general employees) to take security issues seriously and engage in the process of protecting the organisation.

The interviewees also highlighted the importance of engaging managers and heads of business divisions and teams in the organisation in the security program. The manager of a business unit will be the best person to ask his/her employees to be involved in the security program. Once the managers understand the type of involvement (i.e. development of policy or risk assessment) and are convinced of the benefit of the task, he/she would help to engage the right people with the needed skills and expertise. Therefore, the role of division managers is very crucial in assisting the security team to involve and engage stakeholders in the security program.

As part of ‘Identify relevant stakeholders’ practice, interviewees stated that organisations should undertake two key activities: (1) Determine the context and the level of involvement, and (2) Establish a good relationship with internal stakeholders.

**Practice1-Activity1: Determine the context of stakeholders’ involvement**

Identifying stakeholders involves determining the context (i.e. the practice area and the particular practices) and the nature of involvement of the stakeholders in the ISM process. All thirty-four participants reported that ISMPs are implemented in a cooperative manner with internal stakeholders. Therefore, determining stakeholders’ involvement and role in the ISMP is vital.

The interviewees stressed the importance of knowing who to involve, when and what they should do, to ensure effective communication with stakeholders and therefore, successful management of the practices areas.

> “it's all about knowing who the key people are in the different teams; be it technical teams, legal, HR; and fraud. Then engaging them according the task we want to perform and the skills they have.”  
> P19_Mng_IR

> “there are people that we need to communicate with within our department or outside the department. It depends on the area you are working on.”  
> P1_Mng_Policy

In the previous quotes, experts in incident response and policy management reported that determining the context and the level of involvement are important to identify relevant stakeholders. In addition, the interviewees provided insight about the management practices in
information security that rely heavily on the involvement of stakeholders, types of stakeholders and the nature of involvement in each practice.

**Practice1-Activity2: Establish a good relationship with internal stakeholders**
Participants indicated that to engage the stakeholders effectively, they establish a good relationship with stakeholders. This activity was mentioned by thirty participants as an important activity to enable better understanding and cooperation between the organisation’s security.

For example, when asked whether establishing a good relationship with stakeholders will have a positive effect in influencing them to participate in the organisation security program, twenty participants (e.g., P30_Mng, P31_Cons, P32_Mng, P7_Mng_Risk, P19_Mng_IR, and P22_Mng_IR) stated that ‘Establish a good relationship with stakeholders’ is an important practice, which they do as part of their duties as security consultants and security managers.

“One of the key areas we focus on is to develop a good relationship with different team...” P1_Mng_Policy

P31_Cons added that as a result of these networking sessions, “I have a significant relationship with the business, legal company secretary teams, communications managers, HR managers.”

P32_Mng remarked that, “One of the skills of a consultant is to get on well with somebody really quickly and get to understand them.”

**IOL-Practice2: Develop communication protocol**
All the interviewees argued that communication between the security team and stakeholders is an essential part of the process of securing the organisation’s assets. They reported that communication takes place at various stages (during development, implementation & maintenance and evaluation) of security practice areas. Therefore, effective communication will contribute significantly to the involvement and engagement of the stakeholders in the organisation’s security program. This will ultimately impact the effectiveness of the security practices.

The interviewees stated that to ensure effective communication they ‘develop communication protocol’. Further, the interviewees reported that the ‘Develop communication protocol’ practice consists of three key activities: (1) Assign the right security personnel to be responsible for communication, (2) Mapping the appropriate method of communication with stakeholders and (3) Conduct training on communication skills for security personnel.
Practice2-Activity1: Assign security personnel to be responsible for communication
This activity involves assigning an employee from the security team to work as a mediator between stakeholders and the security team. So, whenever the security team wants to convey a message whether it is about an incident or getting feedback on security policy, the person who is assigned for communication will be asked to contact the stakeholders and deliver the message. In the same way, stakeholders’ feedback and input will be provided to this person to deliver to his/her team. This activity was reported by twenty-seven participants in relation to all ISMP areas. For example, P19_Mng_IR indicated that:

“Actually, normally what happens whenever there is an external communication, it really goes through one single designated person in the team”

The “external communication” term in the previous quote from P19_Mng_IR refers to any communication between the security team and other teams inside the organisations.

In the policy management area, P1_Mng_Policy also reported that all communication with stakeholders and the policy development team should go through him as a manager of the process. In addition, P18_Mng_ISTA argued that assigning the right personnel for communication helps in delivering the message to the right person in either way of communication (from and to the security team).

“With the direct communication, this is sometime a problem, they might route the request to a wrong person. This middle man normally knows how to get a response from a technical team and to whom he needs to contact to get the response.”

P18_Mng_ISTA

Practice2-Activity2: Mapping the appropriate method of communication with stakeholders
For effective communication, the experts argued that the appropriate communication methods should be selected according to the situation and the type of involvement. Several communication methods are used, such as: one to one meeting, group discussion, briefing, email, intranet and phone. This activity was reported by twenty respondents in the relation to ISMP areas.

P2_Cons_Policy for example, stated that he communicates with stakeholders by email, phone and face-to-face meeting. P3_Cons_Policy stated that some organisations use internal social media network such as Yammer for communication between security team and stakeholders.

“there should be a defined communication protocol. One communication protocol that I’ve seen in an organisation social media networks like Yammer. There’s a
According to P22_Mng_IR the type of communications also depends on the preference of the organisation. Some organisations may prefer face-to-face communication while others favour email or by phone. Therefore, the security manager should understand and discuss with stakeholders the preferred methods of communication.

In some organisations, there are regular meetings (i.e. fortnightly or once a month) between the security manager and other stakeholders.

“There are some structured meetings where I meet certain groups or individuals once a month at a certain time. There’s enough interaction going on that we formalized the meeting structure.” P19_Mng_IR

Several participants (e.g., P30_Mng, P31.Cons, P33_Mng_IOL) also mentioned that in their organisations, the security manager will also participate in other teams’ meetings.

Practice2-Activity3: Schedule training on communication skills for security personnel

Twenty-four participants stressed the need for training for security personnel on communication skills. Communication skills include presentation skills, negotiation and using non-technical language which are required to communicate effectively with various stakeholders.

For example, one issue reported by several participants is that there are many stakeholders (i.e. business owners and executive managers) that find it difficult to understand technical terminologies. Subsequently, when the security team communicates with stakeholders using technical language, the message will not get across to them. This will impact their understanding of the security issues and ultimately their involvement and engagement in the security practices.

“The challenge is getting IT and information security to communicate what the business wants to know in a business context. Because often, if you look at it from an IT perspective.” P7_Mng_Risk

P5.Cons_Policy added that using a common language during the communication has a positive effect on the engagement of the stakeholders in the process.

“If that’s put into context the business can understand, they’re more likely to be engaged and actually provide funding to get that project up to mitigate the risk.”

Therefore, participants reported that organisations conduct general training sessions and workshops for all employees (including employees in the security department) on communication skills. In addition, there is specific and targeted training sessions for security personnel.
specialists on soft skills, including how to communicate information security risks in a common business language

“In my organisation we have many professional development seminars and workshops addressing many topics including communication skills”

P17_MngISTA

9.4.2 The Implementation & Maintenance Stage
This section presents data related to practices undertaken to implement IOL management practices. In this stage, all thirty-four interviewees reported one main practice: (1) Managing communications with stakeholders. The following sections discuss this practice and its key activities.

IOL-Practice3: Facilitate communications with stakeholders
It was generally agreed amongst all interviewees that two-way communication between the organisation’s security team and internal stakeholders is vital to ensure the effectiveness of the security program. As part of ‘Managing communication with stakeholders’ practice, the interviewees reported two key activities: (1) Providing feedback and security reporting to other functions, (2) Soliciting stakeholders’ feedback and (3) Prioritising and consolidating stakeholders’ views in light of business needs

Practice3-Activity1: Providing feedback and security reporting to other functions
Interviewees stated that communication with stakeholders involves providing feedback and expert opinion about business process and projects that the organisation is planning to implement. Several examples were given by the interviewees on how they were asked to provide feedback on business process from security perspectives. Further, several interviewees (e.g., P6_Mng_Risk, P7_Mng_Risk and P16_MngISTA) indicated that in their organisations, security managers must be involved in every project where risk assessment is conducted to ensure security requirements are identified and fulfilled.

“Whenever they [business owners/executives] want to do something outsourcing or taking something to the cloud the business has to come to security asking about various things and how to do it. [...] if a business has a requirement for a particular process and want an IT system for that. Our security team has to be involved to ensure that whatever system is implemented should meet certain security requirements” P30_Mng
Practice3-Activity2: Soliciting stakeholders’ feedback

Stakeholders’ feedback and inputs to the information security management process contribute significantly to the success of the process. Soliciting the stakeholder feedback aims to ensure that security practices are clearly aligned to stakeholder and business needs. Therefore, there is overwhelming agreement between the participants on the importance of providing the opportunity for stakeholders to express their view about the security process.

“asking feedback from them [stakeholders]; that's very important because it helps us to build the entire security strategy for the organisation and align it to the business” P33_Mng_IOL

P34_Cons_IOL who is a consultant explained that after suggesting solutions for a specific security problem, he would discuss these solutions with stakeholders and ask them about their feedback.

“we develop different solutions to overcome those challenging. Then we discuss the proposed solution or different options, we tell them these are the option what do you suggest? What is your input in these options?”

Stakeholders’ input in the process is highly important, because they have better understanding of the business process. So, when stakeholders are given the opportunity, they will explain the challenges and problems, they are facing in regards to information security.

“They [the stakeholders] are telling what the problems are, where the problems are and what we need and what we don’t need. There should be a feedback mechanism up in the hierarchy to see what we need to do” P33_Mng_IOL

P16_Mng_ISTA gave an example of one platform in his organisation, where stakeholders can provide feedback, input and participate on the strategic planning of information security in his organisation. They formed “the Business Review Group” which consists of “senior leaders from across the organisation”. The aim of this group is to give the opportunity to senior leaders “to provide input into our strategic planning”. This group meets regularly. In each meeting, the Chief Information Security Officer will “provide an update on our strategy for security and seek input back from the business leadership team across the entire enterprise”

In the previous example, P16_Mng_ISTA also indicates that the CISO of the organisation is showing stakeholders how their feedback has been incorporated in the plan. In this way, the stakeholders are ensured that their input and feedback has been taken into consideration

“So, using that as a process to validate that we are addressing their concerns and to help them understand the types of capabilities that we are trying to improve to protect their business.”
Similarly, P18_Mng_ISTA stated that they have “a global working group”. This group also consists of “representatives from each of those key groups involved, so that we have their ongoing feedback throughout the year and also so that we can provide them insights into what’s coming up and give them the opportunity to drive that in terms of what is going to work best for different groups.”

**Practice3-Activity3: Prioritising and consolidating stakeholders’ views in light of business needs**

This activity was mentioned by twenty participants. For instance, several participants (P1_Mng_Policy, P3_Cons_Policy and P4_Mng_Policy) mentioned that during the development of security policy or the implementation of security controls, there may be disagreement between the security team and the relevant stakeholders in certain issues. Therefore, the security manager must prioritise and consolidate between stakeholders’ views. This is done by trying to find balance between achieving the business needs and fulfilling the security requirements.

> “when there are sort of disagreement and conflicting opinion between us and stakeholders on for example the implementation of controls, I think the solution is not to stop people from being able to do certain things. We need to provide an opportunity for people to do those things in the right way. So we try to reach a middle point where security requirements are met and the business can function.”

*P1_Mng_Policy*

Participants emphasise the fact that they have to remain focused on achieving the business goals and objectives. The concept of being a ‘business enabler’ has appeared in almost every interview. The participants pointed out on many occasions that the ultimate goal of security is to assist the business to achieve its objectives. P5_Cons_Policy provided a case example where a compromise decision was reached between the stakeholders and the security team.

> “they[stakeholders] want to launch a new website for the customer I found some issue I want to fix it. Then we agreed with the stakeholders to do a partial release not a full release and continue Monitor. Then when we fix all the issues it later and allow them to launch the full version of the website. I can’t stop the business; security has to be a business enabler not to show stopper”

**9.4.3 The Evaluation Stage**

This section discusses practices related to the review and evaluation of IOL. One key practice was supported by the data is ‘measure the effectiveness of communication’
IOL-Practice4: Review the effectiveness of communications between other part of the organisation and the security team

Twenty-five participants stressed the importance of evaluating the effectiveness of the communication strategies. They stated that it is very difficult to measure/quantify the effectiveness of the communication between other parts of the organisation and the security team. However, the analysis of the data uncovered that there are two key activities that can be implemented as part of the ‘Measure the effectiveness of communication’ practice: (1) Identify indicative success metrics of how well security issues are communicated and (2) Measure the level of engagement of employees in security practices.

Practice4-Activity1: Identify indicative success metrics of how well security issues are communicated.

Although the participants acknowledged the difficulties of measuring the effectiveness of the communication process with stakeholders, they outlined several indications about the effectiveness of communication with stakeholders. These success metrics or indicators include getting sufficient funds, cooperation and understanding of stakeholders, the level of awareness about the importance of security. Observing the abovementioned indications would provide some sense about the effectiveness of the communication.

In response to the question ‘how do you know that your communication with the stakeholders is effective? P33_Mng_IOL stated that:

“It's a very good question. It's a very difficult thing to get a metric on. So the way I guess we do it is by how many incidents are we seeing? How many when we do phishing? We might send out a deliberate phishing exercise that we're looking to see how many people will click on a link or open a file. We can get a bit of a sense of how well the message is being communicated and understood. And perhaps specific areas that we need to work on even harder to get that message across.”

In the previous quote, the expert indicated that they may apply simulation for a phishing attack to determine whether the employees are aware of this particular risk. Their responses to this exercise may be used as an indication of the effectiveness of communication about risk through ISTA program.

Another indication of the success of the communication process is the support of top management. Participants (e.g., P30_Mng, P31.Cons, P32_Mng) placed a great emphasis on the need for top management support as the main stakeholder in the organisations. They reported that when the top management is aware of the security issue, they will sometimes initiate contact with the security manager or chief information security officer and question whether the
organisation is secure against cyber threats and what are the countermeasures in place to protect the organisations. This initiative from top management indicates that the security team has successfully communicated with the most important stakeholders in the organisation.

“Many times, what happens is that the top management will call me and say that what we need to do. They must have seen incidents that have happened in Australia or across the world and this is a very good sign that our message is getting across to our employees” P13_MngISTA

Practice 4-Activity 2: Measure the level of engagement of employees in security practices

Once metrics are identified the organisation needs to monitor those metrics continually and review them to measure the effectiveness of the communication with stakeholders. Fifteen participants reported that ‘Measure the level of engagement of employees in security practices’ is one of the activities that should be performed to determine the effectiveness of the communication with stakeholders.

The participants stated that close monitoring and review should be undertaken of the identified metrics to determine how well security issues are communicated. This includes checking the response and cooperation of the stakeholders during communication regarding security issues. It also includes the support of executive management and awareness of the role of information security in enabling the organisation to achieve its business strategies.

9.5 Final Validation

To perform the final validation of the information security IOL framework an email was sent to all thirty-four participants to provide feedback on the framework and comments on whether the practices and key activities are comprehensive. Seventeen participants responded to the email with their comments and feedback on the framework.

On response to the question whether communication with stakeholders is actively planned for or done in ad hoc basis. All respondents stated that most of aspects of the communication with stakeholders are done in ad hoc manner.

“On the Practice level, these actions are considered but generally on an activities level not addressed well strategically but rather on an ad hoc basis. Typically, teams don’t have the luxury or time to prioritise soft skills such as communications and relationship building proactively and in some cases, the aptitude may not be there. These things typically develop over time and success varies wildly as a result.” P33_MngIOL
“These are things normally done in an ad-hoc basis from experience, however they will benefit from following a more structured approach and planning, as detailed by this framework.” P19_Mng_IR

“Some aspects are actively planned for (security reporting, communications training and engagement levels), others can be” P8_Mng_Risk

“Generally, this is a formal framework for what is done on an informal, and so ad-hoc, basis” P1_Mng_Policy

One participant indicated that the size of the organisation plays a role as to whether the communication process is done in a formal approach or ad hoc. The participant stated that “For the size of our business ad hoc works better. I can see that larger organisations would need more structure such as this but smaller ones don’t.” P10_Mng_Risk

There was overwhelming consensus amongst all seventeen participants that IOL practices should be actively planned and should be an acknowledged area of security practice that security managers need to focus on.

The stuff of dreams!! Of course, a communications strategy should be a pillar of a security practice. It doesn’t have to be complicated, just thought through and nominated stakeholders taken on a journey in terms of the role they need to play which of course varies depending on whether they are general staff or a project manager, developer, etc. P9_Mng_Risk

“Certainly, needs to follow a more formal and organised approach (as opposed to ad-hoc), it is an area that require considerable improvement.” P15_Mng_ISTA

“it should be an acknowledge area of security and information security manager need to focus on” P33_Mng_IOL

“It should be acknowledged area of security practice, which not only security managers, but also management needs to focus on. A good liaison is required between Information Security, Internal Audit, Compliance and Risk Function.” 4_Mng_Policy

“I think it would be helpful to formalize this approach, as with formalizing other aspects of methodologies used. This is not a priority to be done.” P21_Cons_IR

The participants were also asked whether they think this framework would be useful for organisations? All seventeen participants were supportive of the framework and agreed it will provide sufficient guidance for organisation to formalise the communication process with stakeholders.

“Yes. It would help to embed the value of effective communications into a security practice as an important pillar for success. Not just something people like me rant about. A strong security culture is dependent on every member of an organisation, meaning a very diverse bunch of people and priorities. An engaging security communications strategy and team provide the best opportunity to breach divides, gain people’s trust and attention and drive better security, which has flow on effects
to other areas including process improvement, reduction of complexity, better productivity, confidence, etc.” P33_Mng_IOL

“Yes, this would be useful to ensure that the communications are appropriately managed and receive the priority and thought required to make them successful.” P7_Mng_Risk

One participant argued that the adoption of the IOL framework will improve the security culture. The participant stated that

“Framework will definitely support organisation to define and plan necessary procedure. This will also improve the security culture and will give an impression that IT security is an important area to focus on” P33_Mng_IOL

There were no suggestions to change existing practices and activities or add more to the existing one.

9.6 Discussion

In light of the aim and the research question of this chapter, this section provides discussions and reflections on the findings of the empirical study.

9.6.1 An institutionalisation of the communication process

The data shows that ISMPs cannot be implemented in isolation from the rest of the organisation and that effective communication is a key to manage ISM effectively by increasing the participation and involvement of stakeholders in the ISM process. ISM literature has focused on the need for the integration of ISM process, the involvement of stakeholders and effective communication. The review process identified a deficiency in the literature on what practices should be implemented in organisations to effectively communicate with internal stakeholders to involve them in the ISM process.

The findings of the review reinforce the argument of several researchers that there is a lack of empirical evidence on organisational and human factors in regard to information security. Werlinger et al. (2009) argue that although the literature identifies that security management require collaboration among stakeholders, there is a lack of guidance on how security managers interact and communicate with other stakeholders within the organisation. Therefore, this chapter addresses the gap in the literature by developing IOL management practices framework to guide organisations on the activities that should be implemented during the security management process. The IOL management practices framework is very important as it enables
ISMPs practices by increasing the effectiveness of communication with stakeholders and hence their participation in ISMPs.

The development of IOL management practices is a significant step to institutionalise the communication process which will enable adequate resources and attention to the process instead of relying on the experience and the judgement of individuals during the IOL process. This institutionalisation responds to the call of several researchers (Puhakainen & Siponen, 2010; Werlinger et al., 2009) that IOL management practices is more than incidental and operational day to day activity. It needs to be recognised as a practice that should be articulated, strategized and planned for.

9.6.2 Communication with stakeholders

ISMP areas rely on inputs and feedback from stakeholders within the organisation during development, implementation and evaluation stages of each area. The participation of internal stakeholders in ISM is vital to ensure effective implementation of ISMPs and ultimately safeguarding organisational information assets. Therefore, the security team needs to communicate with relevant stakeholders within the organisation to motivate them to participate, share their knowledge, comply with policy, report incidents and assist in the risk management process. The literature highlights the need for effective communication with stakeholders to undertake ISMPs with different areas (see section 9.2.1).

Ellyard et al. (2002) highlighted common reasons in communication breakdown: (1) the message does not reach the receiver and (2) the receiver misunderstands the message. The first reason has to do with the communication methods used to send the message (face to face, email, phone …etc.) which must match the audience preferences and the culture of the organisations. The second reason for communication breakdown focuses on the way the message is presented. In the security context, the difficulty of communication with stakeholders in the language they understand has been discussed in the literature and by the interviewees in this study. Failing to talk with stakeholders in a common language that they can understand can cause a communication breakdown. Therefore, experts recommended avoiding technical terms and jargon when communicating with stakeholders to enable them to understand the intention of the practice and involve the participant effectively.

Moreover, the identification of IOL management practices improves communication with stakeholders because it guides organisations on the practices they should do to communicate
effectively with stakeholders. ‘Develop communication protocol’ is one of the main practices of IOL. It includes three key activities: (1) Assign the right personnel to be responsible for communication, (2) Mapping the appropriate method of communication with stakeholders and (3) Conduct training on communication skills. This section discusses these activities in relation to existing literature.

By assigning the right security personnel to be responsible for communication, the organisation ensures that there is a central point for communication who can understand both technical and business language. They work as mediator between stakeholders and the organisation’s information security team so both parties can understand each other. In some organisations, the management of information security training and awareness program is usually delegated to an employee with no IT or information security technical background, so they can understand the message that the security team trying to get across and deliver it to the stakeholders. The second activity is ‘mapping the appropriate method of communication with stakeholders’ to ensure the right methods of communication is used so the message can reach the receiver in timely manner. The last activity is conduct training on communication skills. As information security personnel should have effective communication skills.

9.6.3 The role of IOL management practices in cultivating a security culture

Over the past decade, the need to develop security culture has received considerable attention from academic researchers and industrial practitioners (Dojkovski, Lichtenstein, & Warren, 2012; Lim, Chang, Maynard, & Ahmad, 2009; Ngo, Zhou, & Warren, 2005; Oost & Chew, 2012). Many researchers argue that security culture is vital for supporting and guiding security practices to influence employee behaviours to protect organisational information (Lim, Ahmad, Chang, & Maynard, 2010; Ruighaver et al., 2007; Schlienger & Teufel, 2002, 2003; von Solms, 2000). Several studies in security culture have reported factors that influence the cultivation of security culture. These factors include top management support, shared responsibility, collaboration and communication, and employees’ involvement. Although these factors have been studied extensively in the literature, there is no clear guidance on how security managers can take these factors into consideration while implementing ISMPs. Hence, the development of IOL management practices provides a significant contribution to ISM and, specifically, the establishment of a security culture. The following sections present the findings relating to
factors that influence the establishment of a security culture and how IOL practices guide the security team in addressing those factors.

9.6.3.1 Top management support and involvement
Several researchers stressed the importance of top management support and involvement in the security management process (Dokovski et al., 2012; Greene & D’Arcy, 2010; Lim et al., 2015; Straub & Welke, 1998). They argued that top management support and involvement are essential for encouraging compliance and influencing employees’ adherence to security policies. Further, (Ruighaver et al., 2007) and Chia, Maynard, and Ruighaver (2002) contend that information security is a management problem and the security culture reflects how management handles this problem. The findings of this research project confirm and extend the literature on the role of top management.

Identifying relevant stakeholders is a key IOL practice that is undertaken across all ISMP areas. One important type of stakeholders is top management. There was overwhelming consensus amongst the participants on the considerable role that top management plays in influencing employees’ behaviour and attitude towards information security, which can affect their participation in the implementation of ISMPs. Therefore, the participants argued that the security team should attain support and enforcement from top management. The findings of this research have provided insights into the context, nature of involvement, and type of stakeholders across all ISMP areas (see Section 9.6.59.6.4). They show exactly the type of involvement that is required from top management. Most importantly, the implementation of IOL management practices provides better participation and involvement from all stakeholders, because they assist the security team to communicate effectively with stakeholders.

9.6.3.2 Employee involvement
Ruighaver et al. (2007) pointed out that involving employees in information security practices has a positive effect on their behaviour and attitude, as it makes them feel responsible. In the same vein, (LaRose, Rifon, & Enbody, 2008) found that when involvement is low, individuals are likely to take mental shortcuts, and when involvement is high, users are likely to elaborate by thinking arguments through, provided they have clear information and are not distracted from reflection. However, Koh, Ruighaver, Maynard, and Ahmad (2005) found there was a lack of employee involvement in security activities.
The findings of this study confirm the argument of Ruighaver et al., (2007), who argued that the lack of collaboration with the stakeholders in security decision-making may often lead to a dangerously narrow focus of security. They further illustrate that the involvement of stakeholders in ISMPs not only desirable but rather essential for effective management of information security program and provides guidance on how stakeholders can be involved in practices of ISM areas.

9.6.3.3 Collaboration and cooperation
The existing literature pointed out that ISMPs are undertaken by a small group of security specialists within the IT department (Fitzgerald, 2007). This is not surprising, as security is still regarded as highly technical, and requires special expertise to deal with it. As information security is a dynamic and multidimensional discipline (Von Solms, 2001), effective implementation of ISMPs require collaboration with all departments to improve organisations’ information security. The findings of this study support the need for collaboration and cooperation with different departments when undertaking ISMPs in the organisation. Further, the data support Ruighaver et al.’s (2007) conclusion that the lack of collaboration with the stakeholders in security decision making may lead to the risk of a narrow view of information security. The findings of this study show that ISMP needs the collaboration and cooperation of various stakeholders from different departments.

9.6.3.4 Clear assignment of role and responsibilities in regard to ISM
The importance of information security responsibilities, including the assignment of the security responsibility, and the formal security structure, in the development of a security culture is well established. Several researchers postulated that security responsibilities need to be clearly assigned to every employee to protect organisational information (Baskerville & Siponen, 2002) (Doherty & Fulford, 2006). According to Dhillon and Backhouse (2001), the proper assignment of security responsibilities may allow employees to carry out their responsibilities properly and expand their own practice. on the other hand, the lack of proper assignment of security responsibilities may affect the protection of organisational information. The findings of this study support the literature and provide guidance for organisations to clearly assign the role and responsibility of stakeholders in regard to ISMPs through practices that require the identification of stakeholders and the level and context of involvement. IOL management practices assist organisations to define clear roles and responsibilities, which contribute to the cultivation of a security culture.
9.6.4 Stakeholders involvement in ISMPs

As discussed in 9.2.1, there is broad agreement on the importance of involving stakeholders in the ISMPs. Academics and professionals argued that information security is a multidisciplinary issue that requires the involvement of multiple stakeholders with a wide variety of skills from different departments within the organisation (von Solms, 2001; Wood, 2004). Several benefits of stakeholders’ involvement were reported in the literature including achieving elevated levels of awareness which will influence stakeholders’ behaviour and attitude towards information security issues. This will affect their compliance with policy and their cooperation and collaboration in undertaken ISMPs.

Although the involvement of stakeholders has been widely discussed in the ISM literature, there is a need to guide organisation on the level of involvement, type of stakeholders and nature of involvement. The findings of this research project support the argument that management practices cannot be undertaken in isolation from other departments (Hu et al., 2007; Wilson & Hash, 2003). Each of the areas that have been discussed in previous chapters requires the involvement of various stakeholders within the organisation. The notion of stakeholders’ participation in the process of information security management has been significantly emphasised throughout the discussion with security experts in chapters 5, 6, 7, and 8. ISMPs depend heavily on the contributions of stakeholders in the organisation. Therefore, the success of other security management areas (policy, ISTA, risk, and incident response) relies on IOL management practices.

In this chapter, one key practice of IOL management is to ‘Identify relevant stakeholders’. It involves two main activities: (1) Determine the context of stakeholders’ involvement and (2) Establish a good relationship with stakeholders.

In terms of the first activity, ‘Determine the context of stakeholders’ the finding of this previous chapter (5-8), provided a detailed description of the ISMPs that need the involvement of stakeholders, the type of stakeholders and the nature of involvement of each stakeholder. The findings around stakeholders’ involvement and extend the literature by presenting a matrix of stakeholders’ involvement are synthesised in Section 9.6.4. This should contribute significantly in the involvement of stakeholders in ISM process as it provides a better guidance on what practices require the involvement of stakeholders and the type of stakeholders as well as the role they play regarding each ISMP.
The second activity which is reported by the study participants as part of identifying the relevant stakeholders is to ‘Establish a good relationship with stakeholders’. This activity is also supported by existing literature. It was discussed in the literature as a factor that influence the involvement of stakeholders is to develop good relationships with stakeholders. According to Markus and Mao (2004) and Taylor et al. (2013) developing good relationships with stakeholders is likely to result in a high level of participant in ISM process, bad relationships on the other hand are expected to yield bad outcomes. Taylor et al. (2013) stated that “establishing good interpersonal relationships with stakeholders and colleagues in general will always help to present assurance programmes as a worthwhile activity.” (p.63) Good relationships enable the security team to understand stakeholders’ needs and ensure they understand the purpose of their involvement. It also prevents conflicts and disputes that may occur during the process and results in hindering stakeholders from participating in the ISM process (Markus and Mao 2004).

9.6.5 Provide further guidance to increase the level of stakeholders’ involvement (stakeholders matrix)

There is an overwhelming consensus amongst academics and industrial professionals on the importance of involving all employees in the information security process. Several researchers (Kandogan & Haber, 2005; Wood, 2004) and practitioners Kissel et al. (2008) argued that information security is a multidisciplinary issue that requires the involvement of multiple stakeholders with a wide variety of skills from different departments within the organisation (von Solms, 2001; Wood, 2004). Several benefits of stakeholder involvement have been reported in the literature, including achieving a high level of awareness that will influence stakeholders’ behaviour and attitude towards information security issues. This awareness will affect their compliance with policy and their cooperation and collaboration in undertaking ISMPs.

Although the involvement of stakeholders has been widely discussed in the ISM literature, there is a need to guide organisations on the level of involvement, type of stakeholders, and nature of involvement. The findings of this research project support the argument that management practices cannot be undertaken in isolation from other departments (Singh et al., 2013). Each of the areas that have been discussed in previous chapters require the involvement of various stakeholders within the organisation. The notion of stakeholders’ participation in the process of information security management has been significantly emphasised throughout the discussion with security experts in Chapters 5, 6, 7, and 8. Information security management practices
depend heavily on the contributions of stakeholders in the organisation. Therefore, the success of other ISMP areas (policy, ISTA, risk, and incident response) relies on IOL management practices.

**9.6.5.1 Policy Management**

In policy management (see Chapter 6), there are four practices, that depend on the involvement of stakeholders: (1) *Determine organisation’s security needs*, (2) *Create security policy document*, (3) *Enforce the security policy*, and (4) *Review security policy*. Each of those four practices has relevant stakeholders that should be involved by undertaking specific duties to ensure the effectiveness of the practices. These duties mainly include providing information about the business process, review and feedback, and support and approval. Table 9-4 presents policy management stakeholders matrix.

**Table 9-4 Policy management stakeholder matrix**

<table>
<thead>
<tr>
<th>Practice</th>
<th>Type of stakeholders</th>
<th>Nature of Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine organisation’s security needs</td>
<td>Top management</td>
<td>Provide inputs to assist the development team/ external consultant in identifying security requirements as they</td>
</tr>
<tr>
<td></td>
<td>Business processes owners</td>
<td></td>
</tr>
<tr>
<td>Create security policy document</td>
<td>Depends on the type of policy</td>
<td>Stakeholders to review the document and provide feedback</td>
</tr>
<tr>
<td></td>
<td>Top management</td>
<td>Approve the final draft and sign it</td>
</tr>
<tr>
<td>Enforce the security policy</td>
<td>Depends on the policy Usually head of divisions/ department For example HR.</td>
<td>Assist in monitoring employees and ensuring they adhere to the policy. Reporting noncompliance Implement disciplinary actions</td>
</tr>
<tr>
<td>Review security policy</td>
<td>Depends on the type of policy Middle Management Employees</td>
<td>Provide feedback about policy</td>
</tr>
</tbody>
</table>

The literature highlights the importance of stakeholder participation in the management process of the security policy and outlines several advantages of involving stakeholders in the process (Doherty & Fulford, 2006; Kadam, 2007; Maynard & Ruighaver, 2003; Maynard et al., 2011; Ølunes, 1994; Rees et al., 2003; Whitman et al., 2001). The findings of this research provide empirical evidence to support the existing literature and offer insight into the type of stakeholders and the nature of involvement in each practice in the policy management process. They also emphasise the conclusions of several researchers (Maynard et al., 2011; SANS Institute, 2001; Siponen et al., 2014; Sommestad et al., 2014) that involving stakeholders has a positive effect on the quality of the policy and the compliance of these stakeholders with it.
9.6.5.2 Information security Risk management

The data show that there are two key practices that depend on the participation of relevant stakeholders: (1) *Establish risk management context* and (2) *Facilitate the risk assessment*. Participants indicated that during both practices stakeholders (senior and line level managers) play a major role in providing inputs to in regard to the business process through participating in seminars, workshop and interviews with the security manager. The interviewee explained that the quality of the risk assessment depends on the quality of the inputs provided by the stakeholders. Further participants indicated that stakeholders are responsible for whether to accept the identified risk or implement a control to treat the risk. Therefore, the study provides evidence on the key role of stakeholders in information security risk management and explains the type of involvement. Table 9-5 summaries the risk management practices, type of stakeholders and nature of their involvement in each practice.

**Table 9-5 Risk management stakeholder matrix**

<table>
<thead>
<tr>
<th>Practice</th>
<th>Type of stakeholders</th>
<th>Nature of Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish risk management context</td>
<td>Senior management and managers of particular areas)</td>
<td>Define goals and objectives of the process</td>
</tr>
<tr>
<td>Facilitate the risk assessment</td>
<td>Senior management Middle management</td>
<td>Provide information about business process, assets, threats, risks, likelihood, consequences and existing controls, Discuss with security team whether to accept risk or implement controls to mitigate risks</td>
</tr>
</tbody>
</table>

Existing literature on the information security risk management process acknowledges the need for stakeholder involvement in the process. Identifying stakeholders is one of the key activities outlined as part of ‘*establish risk management context’*, because it is believed that it enables the organisation to communicate with those people and encourage them to participate in the security risk management process. The findings of this study reinforce the conclusion of the Spears and Barki (2010) study on user participation in information security risk management which support the importance of involving users in the process of managing security risk. Spears and Barki (2010) argued that the participation of users has a positive effect on security risk management. The involvement of users provides needed knowledge of a business process, which will result in “*greater alignment between information security risk management and business environment*” (p.503). The alignment will improve the information security risk management and, as a result, enable the organisation to implement effective security controls to mitigate risks.
9.6.5.3 ISTA management

The data show that the involvement of stakeholders is vital to these three ISTA practices: (1) *Conduct needs assessment*, (2) *Develop ISTA materials*, and (3) *Review ISTA program*. These practices rely on feedback and input from the stakeholders (see Table 9-6). Therefore, these practices should be undertaken in cooperation with different stakeholders. The findings support the literature and provide further evidence and explanation on how stakeholders are involved in the process.

**Table 9-6 ISTA management stakeholder matrix**

<table>
<thead>
<tr>
<th>Practice</th>
<th>Type of stakeholders</th>
<th>Nature of Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct needs assessment</td>
<td>Head of divisions</td>
<td>Provide feedback on the needs for ISTA</td>
</tr>
<tr>
<td>Develop ISTA materials</td>
<td>Head of divisions</td>
<td>Participant in the development and provide feedback on the material, delivery methods</td>
</tr>
<tr>
<td>Review ISTA program</td>
<td>Head of divisions, Participants in the program (e.g., employees, and managers)</td>
<td>To ensure that ISTA program is effective, ISTA team collect feedback from employees about the program.</td>
</tr>
</tbody>
</table>

9.6.5.4 Information security incident response management

In the ISIR management area (Chapter 8), the data demonstrates that stakeholders play an important role in responding to information security incidents and provide feedback and reflection as part of the lessons learnt from incidents. Therefore, that there are two incident ISIR management practices that rely on the participation of the stakeholders: (1) *Facilitate incident response activities* and (2) *Facilitate lesson learnt from incident* (see Table 9-7).

**Table 9-7 Incident response management stakeholder matrix**

<table>
<thead>
<tr>
<th>Practice</th>
<th>Type of stakeholders</th>
<th>Nature of Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilitate incident respond</td>
<td>Relevant stakeholders include employees with technical capabilities to deal with an incident as well as managers, people who are affected by the incident</td>
<td>Participate in the incident response team. Team will be formulated from relevant stakeholders based on the nature of the incident and the roles and responsibilities of the stakeholders. Perform the incident response lifecycle</td>
</tr>
<tr>
<td>Facilitate lesson learnt from incident</td>
<td>Stakeholders who were involved in responding to the incident</td>
<td>Participate in meeting to review and discuss activities undertaken to respond to a security incident. Provide recommendations such as updating security policy, change technical controls configuration and providing awareness and training program.</td>
</tr>
</tbody>
</table>
These findings are aligned with existing literature in the area. Ruefle et al. (2014) and Ahmad, Hadgkiss, et al. (2012) argued that incident management can involve various parts of an organisation, because the current level of complexity of security incidents requires a variety of skills and knowledge to respond to those incidents, thus preventing and minimising their impact (Hove & Tårnes, 2013; Tøndel et al., 2014). Therefore, ISIR process depends on the involvement of different stakeholders as it cannot be performed apart from the rest of the organisation.

9.6.6 Evaluating IOL management practices
Measuring the effectiveness of communication is very important. Participants report on two activities that they undertake to determine whether the communication with stakeholders is successful. These activities include ‘identify success metrics’ and ‘monitor the identified metrics’. The experts indicated that it is very difficult to measure and quantify the effectiveness of the communication process with stakeholders. However, they state that they can sense that the communication was successful in terms of support and involvement of top management, level of awareness, the initiation of contact from stakeholders with the security team, and the number of incidents caused by employees. Although the data shows that information security managers are paying attention to whether their messages are getting across to the rest of the organisation, it seems that the evaluation process is not formal and well established. There is a clear gap in the literature and in practice with regard to the best way to measure the effectiveness of communication. Future work could look at the management and communication literature in this area to identify methods and theories to measure the effectiveness of internal communication with stakeholders.

9.7 Summary
This chapter presented the development of information security intra-organisational liaison (IOL) management practices framework based on the findings of this research project. It started by introducing IOL and its importance to enable ISM practices. Then, an overview of the literature in IOL in information security management literature is presented; highlighting gaps and deficiencies in the area. Then, a framework was developed based on the analysis of the empirical data. The chapter ended discussion of the finding from the empirical data and outline of the contribution. The next chapter will present an overall discussion of this research project.
10.1 Introduction

Chapters 5 to 9 presented the development and validation of the framework of information security management practices (ISMP) within five areas of information security management (ISM): risk management, policy management, information security training and awareness (ISTA) management, incident response management, and intra organisational liaison (IOL) management.

This final chapter discusses the overall results of the study. The chapter revisits the aims of this research and elucidates how the findings of this research have answered the research questions. It then discusses the main contributions of this research for academic researchers and security practitioners alike by discussing the significance of these contributions to both IS security research and organisational information security management practices. The chapter also highlights the limitations of this research and opportunities for further research. Then ends with conclusion and final remark section.

10.2 Project Overview

The conduct of this research was motivated by the lack of coherent and comprehensive guidance on ISMPs that should be implemented in organisations. Such guidance is extremely important for managing information security programs effectively in a very complex risk landscape.

Considerable work has been done by both academics and practitioners to improve the security posture of organisations. This effort has resulted in frameworks, guidelines and recommendations being proposed for what organisations should implement to protect information resources. However, three deficiencies have been identified in the literature (see Section 2.4). The three deficiencies are (1) poor conceptualisation around ISMP, (2) lack of comprehensive guidance on ISMPs for organisations, and (3) lack of empirical work in the ISM area, more specifically in managerial practices. The three deficiencies identified constitute
different aspects of a common problem: namely the lack of comprehensive, coherent and empirically tested guidance for organisations on information security management practices.

A qualitative research approach was adopted to enable the researcher to gain an in-depth understanding of the research phenomena and develop a framework that could be used to address the problem of insufficient guidance to organisations on ISMPs. Next, the researcher examined several theories from different disciplines to find a theory that could be used as a lens to guide the investigation of the phenomena. The systems theory was found suitable to understand the context of ISM with the organisation and the relationships between ISMP areas. However, no theory was found to explain how ISM is practiced; therefore, it was decided that a synthesis of the body of knowledge on ISM would be the most appropriate way to achieve the objectives of this research.

Next, a comprehensive review and analysis of the ISM literature was conducted to develop the preliminary framework of ISMPs. The review and analysis of the literature was conducted in two rounds. The first round of the review used general search terms to identify ISMPs in the literature, and resulted in the identification of four areas of ISMP. The second step of the literature review and analysis focused on the analysis of the literature of each of the ISMP areas. This resulted in the development of an ISMP framework for each area.

Empirical data were then collected to refine and validate the proposed conceptual framework by conducting interviews with information security management practitioners (consultants and senior and middle-level management). The data collection involved two sequential rounds. First, thirty-four semi-structured interviews with security experts were conducted to refine the ISMP framework of each area. The data obtained were analysed using coding techniques (open, axial and selective coding). New themes were mapped to refine the model. Second, the refined frameworks of each ISMP area were then sent to the participants of the first round to provide comments and feedback. The participants’ feedback and comments were incorporated for the final validation.

The final framework of information security management practices (see Table 10-1) provides a high-level answer to the research question, “How can information security management be practised in organisations?”. The framework of each ISMP area consists of Development stage, the Implementation & Maintenance stage and the Evaluation stage.
The findings from the conceptual study and empirical study of this research project resulted in the development of a framework of ISMP to address deficiencies identified in the literature review. The research framework of ISMP makes significant contributions to theory and practice by providing organisations with guidance on managing their information security program in a more systematic and holistic manner. In this section, answers to the primary and supporting research questions guiding this project are provided.

### 10.3 Answers to the Research Questions

The findings from the conceptual study and empirical study of this research project resulted in the development of a framework of ISMP to address deficiencies identified in the literature review. The research framework of ISMP makes significant contributions to theory and practice by providing organisations with guidance on managing their information security program in a more systematic and holistic manner. In this section, answers to the primary and supporting research questions guiding this project are provided.

#### 10.3.1 Primary research question: How can information security management be practised in organisations?

The review and analysis of both academic and professional literature uncovered that there is a need for consistent, coherent and comprehensive guidance on ISMP for organisations. Three deficiencies were identified in ISM literature (see Section 2.4). This section explains how the three deficiencies identified are addressed and therefore, the main question of this research is answered.
The first deficiency is *poor conceptualisation around ISMP*. The literature of ISM does not have a clear definition of ISMPs and what it constitutes. This has led to inconsistencies in both the academic and professional literatures when referring to ISMP, with the range of ISMPs varying with different researchers and institutions. Further, the immaturity in the discourse has also resulted in the lack of agreement on the levels of granularity in management activities.

The development of the ISMP framework addresses the first deficiency identified in the literature. The ISMP framework is developed through rigorous synthesis and analysis of the literature. The framework provides a clear and consistent classification of ISMPs. It also provides guidance to organisations on the managerial level practices. The ISMP framework consists of practices and key activities of six areas: risk management, policy management, information security training and awareness (ISTA), incident response management, and intra organisational liaison management. The practices and key activities of each ISMP area, are classified into three institutionalisation stages: Development stage, the Implementation & Maintenance stage and the Evaluation stage.

The proposed ISMP framework provides a useful complement to industrial standards (e.g., ISO/IEC 27001 and NIST) giving further guidance to organisations on the range of ISMPs that should be implemented and how those practices are applied in different organisational contexts. Organisations seeks advice from industrial standards to manage their information security programs (Al-Ahmad & Mohammad, 2013; Nykänen & Hakuli, 2013). Although the development of the standard has played a considerable role in building organisations’ information security program, and continuous updates and improvements have been made to the standard since it was first developed, scholars and practitioners point out two main deficiencies in the standard (Siponen & Willison, 2009). First, the scope of the application of the current standards appear to be very generic as they do not consider the specific requirements of organisations (Siponen & Willison, 2009). Second, practices within the standard are not backed by empirical data. Siponen and Willison (2009) stated that “The international ISM guidelines being considered were based on ‘generally accepted principles’, or ‘best practice’. Neither the evidence for the reasoning behind them nor the underlying research processes were given or made public and visible. Thus, the results are not verifiable or repeatable. Thus, practitioners have no way of evaluating the reliability (or objectivity) of the claimed best practices.” (p.269).
To overcome the generic nature of current ISM standards and guidelines, the proposed ISMP framework provides further explanations of how ISMPs are implemented by organisations of all sizes, industries, and jurisdictions. This explanation has been provided by the information security management experts (security managers and security consultants) who were interviewed as part of the validation and refinement for the proposed ISMPs framework. This application to a range of organisations has made the practices and activities in the ISMP framework more adaptable to different organisational needs. Therefore, this research project was able to provide guidance to various types of organisations on the implementation of ISMPs, and, thus, the ISMP framework complements current standards and guidelines.

Further, the ISMP framework focuses on the strategic level activities undertaken by the organisations to secure their information resources. The practice in the standards, however, includes strategic-level (managerial) and technological-level. Therefore, the ISMP framework provides further guidance for organisations on the managerial practices of information security that should be implemented in organisations.

There are many practices in the standard that are implicit, they have been made explicit and comprehensive by the proposed ISMP framework. For instance, one of the main sections in the standard is information security policy. The objective of this section is, as outlined in the standard “to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations” (ISO/IEC 27001, p.2). It also consists of two parts: information security policy documents and review of the information security policy. Each part encompasses a description of the controls and a guide to the implementation. However, the implementation guidance does not explicitly provide direction for the practices and activities that should be performed to effectively implement the controls suggested by the standard. Rather it gives very high level guidance. For example, the standard explains the structure of the information security documents and what they should contain, but does not discuss managerial practices such as formulating the policy development team, identifying the security requirements, and how the policies are communicated and enforced.

The second deficiency is the lack of comprehensive guidance on ISMPs for organisations. Several researchers have cited the lack of comprehensive work in the ISM area and the need for a holistic and comprehensive approach (Lim et al., 2012; Soomro et al., 2016; Zafar & Clark, 2009; Zafar et al., 2014). Much research has been published on managerial-level security practice such as policy, risk, awareness and incident response however the literature is
fragmented and does not investigate the collective management practices that organisations should institute for information security purposes (Choobineh et al., 2007). In addition, effective implementation of ISMPs requires a firm understanding of the interdependence and relationships. The understanding of interdependencies enables ISMPs to be implemented in collective and holistic manner achieving synergy and integration between ISMPs.

The proposed ISMP framework and the identification of the interdependencies between ISMPs in this research (see Section 10.3.2), addresses the second deficiency. It is an important step to provide comprehensive guidance to organisations on the managerial practices of information security and how they can be implemented in a holistic and collective manner. Consequently, ensuring high level integration and synergy between ISMPs and hence, an effective management of information security in organisations.

The third deficiency is the lack of empirical work in the ISM area more specifically into the managerial practices. The proposed ISMP framework is empirically validated and refined through two rounds of semi-structured interviews. Empirical data has provided in depth understanding of the range of ISMPs implemented, how they are implemented in different organisational contexts and the relationships and interdependencies between them. This addresses the third deficiency.

Following two sections outline the answer for the two supporting questions which enabled the answer of the primary research question.

**10.3.2 Supporting research question 1: How are Information Security Management Practices related to each other?**

The findings of this study assist organisations to achieve a holistic implementation of ISMPs by identifying the relationships between ISMPs and understanding the interdependencies between ISMPs. The findings address the second deficiency in the literature, which is the lack of a comprehensive approach to ISM. The identification of the relationships and interdependencies between ISMPs is of high significance to the successful management of ISM in organisations, because the knowledge of the interdependencies assists organisations in making an informed, educated decision or judicious selection about which ISMPs are required to meet their information security requirements. Organisations will be able to know the flow-on effect of implementing one practice and the impact of not selecting or selecting a particular practice on the overall information security program.
As discussed in Section 3.2.3.1, the systems theory was used to guide data collection and analysis to identify relationships and interdependencies between information security management practices. The systems theory approach provided a better picture of the network of subsystems and interrelated parts that form a complex whole (the ISM). After the ISMP areas were identified and the preliminary framework of each area was developed, the researcher was guided by systems theory when identifying connections between ISMP areas (subsystems of ISM). Although several studies have pointed out the interdependencies between ISMPs, the discussion of the interdependencies is presented at a very high level of granularity and there is little empirical evidence of these interconnections and whether security managers pay attention to them (Mitnick & Simon, 2011; Schneier, 2011; Torres & Sarriegi, 2004). Therefore, during the data collection the researcher asked participants a range of questions around inputs to ISMPs and the relationships between ISMP areas. The analysis of the empirical data through the systems theory lens helped to identify relationships and interdependencies between ISMPs (see Figure 10-1).

The significance of understanding the interdependencies between ISMPs. Identifying the relationships between ISMP areas can be summarised into three main points.

First, an organisation conducting an audit may find that they have implemented some ISMPs but not others despite the clear interdependencies (see Figure 10-1). A clear mapping of the interdependencies (such as in Figure 10-1) enables organisations to identify any flaw in the logic, planning and strategies related to ISMPs. Therefore, the framework of interdependencies serves as a means to assure whether strategies are complete and comprehensive.

For example, the findings showed that risk management provides inputs to policy, ISTA and incident response. Also, incident response provides inputs for risk management, policy and ISTA. Therefore, the quality of one practice can affect other practices. In this example, the quality of risk assessment results should lead to an accurate identification of the information security requirements, which should then result in developing a relevant policy that fulfils the organisation’s information security requirements. On the other hand, inaccurate risk assessment will eventually lead to poor quality policy that does not reflect the actual information security requirements.

Second, knowledge of interdependencies influences planning and decision-making in information security. Depending on the information security requirements of an organisation,
and the available resources, organisations determine which ISMPs must be implemented and which ones might be implemented depending on available resources.

The framework of interdependencies (Figure 10-1) is very useful in providing a much better and accurate cost estimation of organisations’ implementation plans, and providing support for the ISMPs that organisations want to implement. For example, the findings show that in order to develop an effective ISTA program, an organisation really needs to conduct risk assessment and develop policies. Without conducting risk assessment and developing information security policies, the effectiveness of ISTA is questionable, as effective ISTA is mainly based on raising the awareness of employees about the risk identified during the risk assessment process, and the management directions and positions that are outlined in the organisation’s policy.

![Figure 10-1 The overall ISMPs dependencies Framework](image)

Third, the awareness of the interdependencies between ISMPs improves the communication and collaboration within the organisation’s information security team, as ISMPs may be conducted by different teams within the security/IT department of an organisation. Knowing the relationships can enable a better understanding of what inputs are needed from one ISMP area
to another, which will improve the interaction and cooperation between those teams. The resulting collaboration will have an instrumental effect on the effectiveness of the ISM process in the organisation. It will also enable the organisation to have a consistent approach to the implementation of ISMPs by considering all ISMP areas.

The interdependencies and relationship between ISMP practices are grouped into three main categories, risk management centred, incident response management centred and ISTA management centred. Each relationship between ISMPs is referred to by the letter ‘R’ and a number. See Appendix B for representative evidence for interdependencies between ISMPs. The following sections will explain these three main categories.

10.3.2.1 Risk Management Centred View of Interdependencies

The findings of this study revealed that information security risk management provides inputs for several practices within ISMPs area. Figure 10-2 depicts five interdependencies, each of them are explained in this section. This section presents the interdependencies between the risk management area and other ISMPs areas.

![Figure 10-2 Risk management centred interdependencies](image)

- **R1**: The risk assessment report informs the development of IR policy

The importance of planning and preparation for incident response is well recognised in the literature (Jaatun et al., 2009; Line et al., 2014; Tan et al., 2003; Tøndel et al., 2014). Effective
incident response depends on having a well-documented incident response plan (Jaatun et al., 2009; Line et al., 2014; Tan et al., 2003; Tøndel et al., 2014). The findings of this research revealed that during the planning and preparation for incidents, it is important to have a recent and accurate risk assessment report. Several participants stated that one of the practices in incident response management area \textit{Create incident response policy} requires inputs from risk management. The risk assessment report will enable the ISIR team to be aware of the type of risks to the organisation’s information resources and therefore, be well prepared to respond to these type risks. Hence, good planning and preparation for security incidents require a recent and accurate risk assessment report.

- **R2:** The Risk assessment report is required to identify the needs for ISTA program

The findings of the study revealed that the risk management area provides important input to the ISTA management area. The data on ISTA management practices shows that the risk assessment report is one of the key inputs to the practice of \textit{conduct needs assessment}. Although, the literature on ISTA mentioned that the ISTA program should aim to raise the employees’ awareness about the threats and vulnerabilities of the system (Hansche, 2001; Peltier, 2005; Wilson & Hash, 2003), to the best of our knowledge, the literature does not refer to the risk assessment report as an input to the need assessment for the ISTA program. When asked about how organisations identify the need for an ISTA program, the participants in this study mentioned the risk assessment report explicitly. Therefore, an accurate risk assessment is very important for developing a relevant and effective ISTA program.

- **R3:** The Risk assessment report is required to review the ISTA program

While the literature on ISTA focuses on the need to evaluate the effectiveness of the ISTA program and ensure it is up-to-date (Maqousi et al., 2013), it does not refer to the use of the risk assessment report (Manifavas et al., 2014). The findings of this study show that a recent risk assessment report triggers the review process and ISTA materials are updated to reflect the current state of risks and raise the awareness about those risks that are faced by the organisations. The participants of this study stated that the risk assessment report is very important input to review and update the ISTA program.

- **R4:** The Risk assessment report is required to determine the organisation’s security requirements
The risk assessment report is considered to be an essential input to one of the main practices of the policy management area: *Determine organisation’s security needs*. Security policy lifecycles tend to show that risk assessment as a practice that should be conducted at the start of the development process to identify security requirements (Bayuk 1997; Gaunt 1998; Rees et al. 2003). Other authors (Kadam, 2007; Whitman, 2008) have a step called ‘requirement gathering’ and ‘documents collection’, where the policy development team examines all relevant documents, including previous policies, risk assessment reports and incident response reports to understand the organisation security needs and requirements.

The findings of this research project reinforce the importance of risk assessment. The participants of this study mentioned that the risk assessment report as a key input to identifying the organisation’s security requirements. Therefore, determining the organisation’s security requirements during the policy development stage depends on the risk assessment report produced in the risk management report.

- **R5: Risk assessment report is required to review the security policy**

There is a wide consensus amongst academics and practitioners on the importance of reviewing and updating policy periodically (Flowerday & Tuyikeze, 2016; Klaic & Hadjina, 2011; Safa et al., 2015). The findings of this study show that the review process of security policy receives input from the risk management area. Information security risks change constantly as a result of changes in the business process, and the environment where the organisation operates. Therefore, it is important to use the risk assessment report as an input to indicate any change in the security requirements that will require policy updates. Hence, the review process of security policy depends on the risk assessment report.

10.3.2.2 Incident Response Management Centred View of Interdependencies

This section presents the interdependencies between the information security incident response (ISIR) management area and other ISMPs areas. Figure 10-3 depicts six interdependencies, each of them are explained in this section.

- **R1: Incident response report is required to establish risk management context**

The practice *Establish risk management context* aims to develop an understanding of the external and internal context for ISRM (Fenz et al., 2014). This includes examining the organisation to determine if there are any industry-specific risks, as well as any other issues that may impact the ISRM process (Shedden, Ahmad, Smith, Tscherning, & Scheepers, 2016). The
findings of this study revealed that the incident response report is very important in establishing risk management context. The study participants stated that they use the incident response report to enable them to develop a good understanding of the organisation by looking at the previous incidents and all related information such as the cause of incidents, type of risks, and what was done to respond to each incident. This is very crucial to develop the ISRM approach to enable organisations to accurately identify assets, threats, and risks, and determine the risk likelihood. Thus, establishing the risk management context and the risk assessment process depend on the incident response report.

Figure 10-3 Incident response management centred interdependencies

- R2: Incident response report is required to review risk management process

Several researchers questioned the effectiveness of current risk assessment methods (Fenz & Ekelhart, 2011; Webb et al., 2014). Webb et al. (2014) argued that current information security risks assessment methodologies are commonly estimated with little reference to the organisation’s actual situation. Their findings support the conclusion of Fenz and Ekelhart (2011) that “current risk management approaches generate solutions based on these uncertain input data” (p.58).
The findings of this study indicate that the incident response report is very useful for improving and assessing the accuracy of the risk management practices. Participants reported that they use the incident response report during the risk assessment process to understand the current threats faced by the organisation. They also stated that the risk assessment report is updated (adding new risks, or changing the rating of existing risks) as they learn from incidents. In other words, incident response report assists organisations to keep their risk register up-to-date. Providing an incident report input can overcome the deficiencies in the current risk assessment methods and result in much more reliable information that the security team can use to build security strategies and justify the need for more investment to protect the organisations. The findings of this study support the argument of Ahmad, Maynard, et al. (2015) that learning from responding to previous incidents can expose inaccurate risk assessment.

- **R3:** The Incident response report is required to identify the needs for ISTA program

The findings of this study show that the incident response report is also very important for identifying the need for the ISTA program. The interviewees stated that whenever there is an information security incident, they would take the opportunity to educate people by developing security training around the incident. In other words, as the organisation learns from incidents, they develop new security training and awareness to make the employees aware of an incident, how it happened, and how it can be prevented from happening again. This finding is consistent with the literature in ISTA where several authors (Vroom & Solms, 2002; Wilson & Hash, 2003) reported that the incident report is used as an input for the ISTA management process.

- **R4:** The Incident response report is required to review the ISTA program

Research on learning from security incidents explains that learning from responding to past incidents can indicate insufficient and/or ineffective ISTA program (Ahmad, Maynard, et al., 2015). The findings of this study revealed that the incident response report is an important input to the review process of the ISTA program. Participants stated that as they learn from incidents, they review the ISTA program and recommend new updates to the current program. In addition, they also contended that the number of incidents would be used as an indicator for the effectiveness of the ISTA program. The literature supports the finding on using the number of incidents to measure the effectiveness of the ISTA program (Hansche, 2001).

- **R5:** Incident response report is required to determine the organisation’s security requirements
The knowledge of past incidents which is provided by the incident response report is also very useful to determine the organisation’s security requirements. Several policy development lifecycles (Kadam, 2007; Whitman, 2008) have a step called ‘requirement gathering’ and ‘documents collection’, where the policy development team examines all relevant documents, including previous policies, risk assessment reports and incident response reports to understand the organisation’s security needs and requirements. The findings of this research project reinforce the importance of the incident response report to identify the organisation’s security requirements. Therefore, determine the organisation’s security needs can be informed by incident response reports.

- R6: Incident response report is required to review the security policy

The importance of gathering information security incident data to inform the policy review process cannot be underestimated. The number and type of incidents can be strong indicators for determining whether the policy is no longer effective (Bañares-Alcántara 2010; Kadam 2007; SANS Institute 2001), which helps to identify areas in the existing policy that must be updated, added, or removed. In other words, it helps to recommend possible changes in the current policy to ensure that the organisation’s security policy remains an effective control for protecting the organisation from the evolving risks’ environment. The findings of this study show that there is a consensus between the participants on the need for the incident response report to review the organisation’s security policy. The participants of this study stated that the policy should be reviewed as they learn from incidents. Security incidents may also trigger the ISP review process providing recommendations and suggestions for improving the policy and keeping it up-to-date. This finding supports the argument of (Ahmad et al. 2015; Park et al. 2012) that learning from incidents can improve the effectiveness of the organisation ISTA program.

10.3.2.3 ISTA management Centred View of Interdependencies

This section presents the interdependencies between the information security training and awareness (ISTA) management area and other ISMPs areas. Figure 10-4 depicts five interdependencies, each of them are explained in this section.

- R1: ISTA program is required to communicate the risk assessment results

An ISTA program is implemented to raise the awareness of the organisation’s employees of information security risks, which have been identified through the risk assessment process.
The findings of this study revealed that once the results of the risk assessment are documented, a final report is developed which is then required to be shared with relevant stakeholders. Participants suggested that results of the risk assessment is communicated through an ISTA program in several ways, including workshops, presentation and other awareness tools. Therefore, the practice ‘communicate risk assessment result’ depends on the ISTA program in organisations.

Figure 10-4 ISTA management centred interdependencies.

- R2: ISTA program is required to prepare for incidents

The findings of this study show that an ISTA program is required to prepare for incidents. The practice ‘create incident response policy’ involves scheduling training for relevant stakeholders to ensure they have the required skills to respond to security incidents. All participants indicated that there should be training on the organisation’s incident response procedures to increase the readiness of the organisation. The interviewees reported that training sessions are conducted in their organisations for employees who may take part in the information security incident response process. These sessions are usually presented as scenario based to assess the readiness of employees and getting everybody aligned with what the procedure says and how to react to
an incident. Therefore, the preparation and planning for security incidents depend on the ISTA program.

- **R3: ISTA program is required to communicate the security policy**

The findings of this study show that ISTA is required to communicate the security policy. The study participants stated that the security policy is communicated through ISTA program. These findings support the literature on the role that ISTA program play to communicate the security policy. Several security policy development lifecycles (e.g., Bacik, 2008; Hare, 2002; Lowery, 2002; Patrick, 2002) include policy communication as one of the main practices. They argue that policy should be communicated to employees through an ISTA program to provide employees with the required knowledge and skills to enable them to comply with security policy (Knapp et al. 2009; Maynard and Ruighaver 2003). In the same vein, Whitman (2008) stressed the significant role that the awareness program plays in keeping policies fresh in employees’ minds. Implementing an ISTA program to communicate policy may include providing training sessions to teach users how to perform the security procedures that the policy requires, and conducting an awareness campaign to raise employees’ awareness about the organisation’s policy.

- **R4: ISTA program is required to enforce the security policy**

The finding of this study also revealed that the ISTA program is important for the enforcement of the security policy. Several studies have been conducted to understand why employees do not comply with policy and explore factors affecting employees’ compliance with ISPs (Hedström et al., 2013; Hu et al., 2012; Siponen et al., 2014; Vance et al., 2012; Wall et al., 2013). One of the main recommendations provided by the authors to aid organisations to achieve better compliance with their ISP. is to implement an ISTA program to assist employees in performing their job securely. The data shows that the development of an effective ISTA program will have a significant effect on the enforcement of the ISP and, therefore, employees’ compliance and adherence to the policy. Hence, the enforcement of security policy depends on the implementation of ISTA program.

- **R5: The development of security policy is required for ISTA program**

The data on ISTA management practices shows that there are several key inputs to the practice of ‘conduct a needs assessment for ISTA program’. One key input is the organisation’s security policy. Participants stated that it is the policy that organisations aim to make their employees
aware of. This finding is consistent with the literature. For example, D’Arcy et al. (2009) stated that ISP should be used as an input to determine employees’ needs for ISTA. Several authors argue that security policy is a prerequisite for the development of the ISTA program because it is the policy that organisations want their employees to be aware of (Hu et al., 2012; Tsohou et al., 2010; Tsohou et al., 2008). The literature also mentioned the need to update the ISTA program to reflect any change in the ISP (Parsons et al., 2014; Tsohou et al., 2015). Therefore, ISTA program depends on the development of the security policy.

10.3.3 Supporting research question 2: To what extent are information security management practices institutionalised in organisations?

The findings provide insight into how ISMPs have been institutionalised and how well they have been resourced within organisations. This research has identified that the implementation of ISMPs in different organisational contexts is approached either formally or in an ad hoc manner. The research participants reported their current and previous experiences in the implementation of practices and activities within each ISMP area. This allows for comparison and contrast of the approaches that the different organisations adopt to the implementation of ISMPs. The findings provided evidence that can be drawn on to identify the differences between the implementation of ISMPs in organisations. Respondents from large organisations reported that they take a more formal approach to the implementation of the ISMPs, whilst in small organisations, ISMPs are dealt with more informally.

There are two main reasons that organisations adopt a formal or ad hoc approach to the implementation of ISMPs. First, ISMPs are implemented to comply with standards and regulatory requirements. Organisations that must comply with standards and regulatory requirements (e.g., The Payment Card Industry Data Security Standard (PCIDSS)) are required to implement several managerial controls (security policies and ISTA program). Those organisations that see managerial controls as a regulatory compliance requirement, rather than a valuable control to protect organisational resources, tend to implement ISMPs using an ad hoc approach. This has a detrimental effect on the quality of ISMPs and, therefore, the effectiveness of the information security program. This finding supports (Siponen & Willison, 2009) argument that complying with security standards does not guarantee the quality of the recommended activities in practice. For example, organisations use CBT to gather statistics of who completed the training and how many times they have done it. This helps to fulfil compliance requirements by showing detail on how many and how often employees complete
training. However, several disadvantages were reported by the respondents, such as the lack of human interaction, low motivation and limited preference and learning style. More importantly, statistics around training completion are not good indications of the employee awareness levels.

Second, variations in the implementation of ISMPs can be attributed to the maturity and size of the organisation as well as aspects of management support and the availability of resources (including time, budget and personnel). Respondents from large organisations reported that they formally implement the set of ISMPs, whilst in small organisations, because of a lack of resources, ISMPs are dealt with more informally and occasionally may not be done at all. Although the data suggested that small organisations usually adopt an ad hoc approach and large organisations tend to have a more formal and structured approach, we cannot generalise this and conclude this is the case for all organisations. A small organisation that realises the importance of ISMPs or is not requirement driven may invest and dedicate more resources to implementing ISMPs in a more formal manner. Likewise, a large organisation that is compliance driven may use an ad-hoc approach.

In terms of the maturity of an organisation, most organisations start by implementing ISMPs to comply with standards requirements and then move towards more formal implementation to improve their information security program. The maturity of an organisation’s information security program is influenced by the length of time the organisation has implemented ISMPs: the longer an organisation has been conducting ISMPs, learning from past experience as to what techniques have worked and what have not worked, the more likely the ISMPs are mature. Additionally, having adequate resources to conduct ISMPs influences the level of maturity of the organisation’s information security program. For example, organisations that have a dedicated team managing ISTA will have more opportunities to improve their ISTA program and to achieve a high maturity level and institutionalised activities. This is because having a dedicated team enables the organisation to leverage learning from past experiences.

The answer of this question represents the first step in developing a capability maturity model (CMM) for ISMPs to assist organisations to assess their implementation of ISMPs. This is significant to enable organisations to identify the extent of the institutionalisation their ISMPs and how to progress from informal (adhoc) implementation towards more formal and structured approach.

The knowledge from the assessment process of the organisation’s current state of their approach to the ISMPs implementation will enable the organisation to increase the effectiveness of
ISMPs. This is can be done by effectively planning and strategizing their implementation of ISMPs by understanding their maturity level and identifying their target level in a similar way to the Systems Security Engineering Capability Maturity Model (SSE-CMM) (Dhillon, 2007a; Siponen, 2002). The SSE-CMM defines five capability levels: Level 1 – Base practices are performed informally, Level 2 – Base practices are planned and tracked, Level 3 – Base practices are well defined, Level 4 – Base practices are quantitatively controlled, and Level 5 – Base practices are continuously improving (Siponen, 2002). Organisations can measure their maturity (L1-L5) regarding the implementation of ISMPs, select the desired level and allocate adequate resources such as establishing dedicated team for each ISMP area, providing training for existing staff, hiring personnel with the right knowledge, skills and ability to achieve the targeted level in the CMM model and therefore implement the practice in more structured and formal approach.

**10.4 Contributions**

This research project has several contributions to theory and practice. Table 10-2 provides a summary of the main contributions of this research and the implications of each contribution on improving the implementation ISMPs in organisations.

**Table 10-2 Summary of the research contributions and the implications of each contribution**

<table>
<thead>
<tr>
<th>Research Contributions</th>
<th>Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>The research provides the most complete, comprehensive and empirically backed framework of ISMPs for organisations</td>
<td>The framework complements fragmented best-practice advice on ISM in industry standards. The ISMP framework provides practitioners with a standardised and formal checklist to benchmark or audit their existing ISMPs or assess their level of maturity. Therefore, implement a more formal and institutionalised ISMPs</td>
</tr>
<tr>
<td>The research identifies the relationships between ISM areas, provides empirical evidence for the relationships, justifies the interdependencies between ISMPs, and explains the impact of inconsistent levels of quality among ISM practices</td>
<td>The interdependencies model assists organisations to achieve a holistic implementation of ISMPs as it enables organisations in making an informed, educated decision or judicious selection about which ISMPs are required to meet their information security requirements</td>
</tr>
<tr>
<td>The research identifies a set of activities (Intra Organisation Liaison (IOL) management practices) undertaken by organisations to increase the level of stakeholder involvement and participation in the ISM process.</td>
<td>The identification of the IOL management practices provides guidance to organisations on how to increase the level of stakeholders’ involvement in information security and therefore, cultivate a culture of security.</td>
</tr>
</tbody>
</table>
10.4.1 Contributions to theory

The main contribution of this research to theory is the explanation of how the systems theory can be applied in the ISM domain. The lack of theoretical foundation in the domain has resulted in the discipline not being able to progress and develop as a research discipline because researchers cannot even agree on basic terminology. Therefore, from a discipline point of view, it is fragmented, it is not cumulative in that authors do not build on each other’s contributions, there is no consensus on foundational principles and concepts and there is no coherent view of ISMPs.

10.4.1.1 The application of systems theory in the ISM domain

This research explains how systems theory applies to ISMPs enabling more comprehensive, holistic and coherent understanding of ‘How can ISM be practiced in organisations?’. The systems theory has had a significant effect on understanding ISM and the context in which ISM operates with an organisation. A system is a collection of parts unified to accomplish an overall goal. The systems theory calls for integration of activities related to particular projects or programs into a separate organisational system (Arnold & Wade, 2015; Reynolds & Holwell, 2010). The effect of systems theory in ISM is that it helps security managers to look at the organisation more broadly and to recognise the various parts of the organisation, and, in particular, the interrelations of the parts (Chikere & Nwoka, 2015; Luoma et al., 2007).

Organisations have often focused on a specific ISMP area, and they may therefore lose sight of the overall objectives of the ISM and the role of individual ISMPs areas in the larger ISM systems. These ISMP areas can better achieve their objectives if they are aware of the ‘big picture’. The systems theory approach provides a better picture of the network of subsystems and interrelated parts that go together to form a complex whole. This approach provides a useful way to conceptualise ISMPs and assist in drawing the boundaries between different related concepts. The systems theory is used in the ISM contexts to integrate the various ongoing activities into a meaningful total system.

The systems theory was first applied at the initial stage of this research where the research was trying to establish a comprehensive understanding of the information security management as subsystem of the organisation as whole. The systems theory at this stage enabled the researcher to understand the phenomenon under investigation (ISM) and its context within the organisation. Then, the systems theory was applied recursively regarding ISM as a system and aiming to determine subsystems that constitute the ISM and the relationships between these
subsystems. The systems theory guided data collection and analysis and helped to identify relationships and interdependencies between ISMPs.

10.4.2 Implications for Practice
This section presents the implications of this research for organisations and security practitioners.

Overall the lack of consensus on what ISM involves and the lack of focus on ISMPs has affected the level of guidance that existing models and frameworks can provide to organisations as the authors have not been able to build on a consistent, coherent explanation of what activity should be implemented and how to implement it. Organisations have no standardized and formal checklist to benchmark or audit their existing ISMPs or assess their level of maturity.

10.4.2.1 Provide practice-based empirically tested framework of ISMPs
The poor conceptualisation and the lack of empirical work in the area have led to conflicting advice and an unclear picture of the domain around what management practices can be implemented in organisations to protect their information resources. Therefore, this study addresses the needs for a comprehensive, coherent and empirically tested information security management practices framework. The framework of ISMPs consists of five areas: risk management, policy management, information security training and awareness management, incident response management and intra-organisational liaison (IOL) management. The first four were identified through the analysis of the literature (Phase 2) and the IOL was identified through the analysis of the collected data from semi-structured interviews. Each ISMP area has a process framework that consists of three institutionalisation stages: the Development stage, the Implementation & Maintenance stage and the Evaluation stage. Each stage involves management practices and key activities. The framework has been refined and validated through two rounds of data collections as part of the empirical study (Phase 3) of this research.

The framework of ISMPs provides comprehensive guidance on information security management practices that can be implemented in organisations in order to manage their information security program effectively. Additionally, the ISMP framework provides practitioners with a standardised and formal checklist to benchmark or audit their existing ISMPs or assess their level of maturity. Security practitioners can use the research framework as a tool to assess an organisation’s current ISMPs. The ISMP framework can also assist organisations to employ personnel with the appropriate skills and knowledge to undertake
ISMPs, as it helps to identify the roles and responsibilities around what organisations need to implement.

10.4.2.1 Provide a more holistic view of the information security management process

Several researchers have cited the lack of comprehensive work in the ISM area and the need for a holistic and comprehensive approach (Lim et al., 2012; Soomro et al., 2016; Zafar & Clark, 2009; Zafar et al., 2014). Lim et al. (2012) argue that although a number of studies do cover individual security ISMPs, none provide a comprehensive overview of these practices. Qingxiong et al. (2008) also recognise the need for a comprehensive list of ISMPs. Several researchers highlight the importance of a comprehensive and holistic approach for information security management (Eloff & Eloff, 2003; Soomro et al., 2016; Swanson & Guttman, 1996).

For example, Dhillon (2007a) argues that an effective security management program should integrate different information security processes, such as undertaking information security risk management, educating personnel in information security awareness and establishing and executing information security policy.

Therefore, the framework of ISMPs provides a more holistic view of the information security management process. The findings explain how ISMPs can be implemented in a holistic and collective manner to ensure high-level integration and synergy between ISMPs and, hence, effective management of information security in organisations. The study has provided empirical evidence for the relationships and interdependencies between ISMP areas. Identifying relationships and interdependencies improves the effectiveness of information security programs as it enables a better understanding of what inputs are needed from one ISMP area to the other. Understanding such information has two main implications. First, it improves the quality of the practices, as the quality of the ISMPs of one area can affect other areas. Second, it improves the communication and collaboration within the organisation’s information security team, as ISMPs may be conducted by different teams within the security/ IT department of an organisation, which will improve the interaction and cooperation between teams. The resulting collaboration will have an instrumental effect on the effectiveness of the ISM process in the organisation. It will also enable the organisation to have a consistent approach to the implementation of ISMPs by considering all ISMP areas.
10.4.2.2 Identification of intra-organisational liaison management practices

The findings of this study revealed that the communication process between the organisation’s security team and internal stakeholders regarding ISMPs tends to be undertaken in an ad hoc and informal manner in organisations. The process in most organisations relies on the experience and the judgement of individuals. Therefore, the development of IOL management practices is a significant step for institutionalising the communication process, which will enable adequate location of resources and attention to the process. It will assist organisations to establish a formal IOL process in order to increase stakeholders’ involvement in the ISMPs. By establishing a formal process for IOL, the communication process will be recognised as a practice that needs to be articulated, strategised and planned for.

This research develops an IOL practices framework that consists of a set of practices and key activities that should be undertaken by security managers to communicate effectively with stakeholders to involve them in the ISM process. The development of the IOL framework addresses the gap in the literature by providing guidance to organisations for enabling ISMPs. In order to communicate effectively with stakeholders and, therefore, successfully implement ISMPs, information security personnel should undertake a set of activities during the information security management process to increase the participation and involvement of relevant stakeholders within the organisations.

The development of IOL management practices provides a significant contribution to the ISM process and, specifically, the establishment of an information security culture, by affecting factors that influence security culture in organisations, which have been identified in the existing literature. The study has outlined strategies to involve stakeholders in the process. It has also developed a matrix of stakeholders’ involvement for ISMPs in each ISMP area. The matrix provides guidance on the types of stakeholders and their level and context of involvement in the information security management practices.

Most of problems in the ISM domain that have been presented in the literature are related to the communication between the organisation’s information security team and internal stakeholders. For example, several researchers argue that the lack of formal communication between the incident response team and the information security management team is the major reason that organisations are not leveraging their experience from responding to security incidents to improve their information security strategies (Ahmad et al. 2012). The fact that people are not talking to each other formally (as it is not institutionalized in culture) and are only talking
informally on the initiative of individuals, points to the fact that IOL management practices are some of the most neglected and most critical practices that researchers are highlighting as being a key reason why security is not successful.

Although the literature provides advice to improve communication between the information security management team and internal stakeholders, there is only fragmented information on the importance of effective communication. This study, however, has holistically identified the need for communication and developed sufficient guidance for organisations to implement a formalised communication and liaison process.

10.4.2.3 Improve the consistency in terminology and semantics

The ISMP framework was developed through comprehensive review and analysis of the literature of the area. This has enabled a synthesis of the knowledge around ISMPs through comparing and consolidating ISMPs in several existing frameworks and guidelines, which have resulted in the development of the ISMPs for each area.

The proposed ISMP framework addresses the problem of inconsistency in terminology and semantics by presenting a clear understating of the terminology that is employed to refer to ISMPs. For example, the ISMP framework for policy makes a clear distinction between ‘communicating’ and ‘distributing’ the security policy. These terms have been used interchangeably in the literature. In the proposed framework, ‘distribute the policy’ refers to selecting the policy delivery methods and doing the actual delivery of the policy documents to the employees, while ‘communicate the policy’ refers to ensuring that the policy has been read and understood by employees. Another example of inconsistency in terminology and semantics is the use of the terms ‘enforcement’ and ‘compliance’ to refer to the effort that management should do to ensure that the policy is adhered to. The model defines ‘enforce policy’ as the management practice that ensures users adhere to policy. Compliance, on the other hand, is the desired result of the enforcement practice.

10.5 Limitations

First, adopting a qualitative approach in this research design has provided an in-depth understanding of the phenomena (ISMPs) through knowledge synthesis and analysis of relevant literature, and also by interviewing the participants (information security managers) in a natural setting. However, since the researcher was the primary instrument for data collection and analysis, research bias is the main limitation of this research design. This is because the presence
of the researcher might influence the behaviour of the participants during the interviews. The researcher’s interpretation of the results might also be influenced by the researcher’s own beliefs, values and prior assumptions. However, according to Walsham (1995), interpretive researchers cannot run away from such biases, as their influence on the participants happens the moment the researcher shares his or her thoughts about the research. To minimise research bias, a training process was conducted to ensure consistency in the process and ultimately enhance the quality of the comprehensive review. Several articles in the research domain were selected by the supervisors and given to the student to review and identify ISMPs. Then supervisors read the articles and list of ISMPs extracted by the researcher and checked whether the researcher had captured all the practices. This process provided inter-rater reliability, ensured that the researcher had a good understanding of the area and also ensured that the researcher also had the ability to identify practices using ISMP definitions. Also, the data collection methods were reviewed several times by the University of Melbourne’s Human Ethics Sub-Committee (HESC) before their approval to conduct the studies was granted.

Second, the scope of organisations involved in this study was very broad in terms of sector, including areas such as education, government, the military and business. The preliminary framework was tested through semi-structured interviews with information security experts from organisations of various types and sizes. However, studies that focused on a specific sector or industry would be able to identify specific practices that are more relevant within that specific sector or industry. Therefore, practices and key activities identified in this study are likely to be generic for all the organisations involved in the study. This has been overcome by explaining how a particular practice is implemented in different organisational contexts.

Third, it was initially planned to conduct multiple case studies in organisations to identify ISMPs implemented in organisations by using multiple sources of data, such as interviews, document analysis and observation. This would have provided insights into how organisations conduct a complex process such as risk management and incident response by interviewing multiple stakeholders. However, this plan was later changed because the researcher could not find organisations that would grant the necessary access. Due to the sensitive nature of information security, most organisations are reluctant to comprehensively expose their information security practices to external parties, including researchers. However, this was less of an obstacle when speaking individually to industry professionals in the context of their past professional experiences. Thus, semi-structured interviews with information security
professionals from various organisations were conducted. This could have limited the quality of data, as only one perspective was taken into account to describe the ISMPs with the areas in an organisation. For example, in the case of a large bank, we interviewed one person who described the information security risk management practices in their workplace. Such a complex process needs more than one person to provide an in-depth understanding of the area and enable the researchers to explain why an aspect of ISMPs is implemented in a certain approach.

The final limitation is the generalisability of this study to organisations in different environmental and organisational structures. Since this research was conducted in Australian organisations, there might be cultural differences that limit the applicability of the findings to organisations in other countries. For example, information security in Australian organisations is highly regulated and compliance driven. This is certainly not the case in developing countries such as in the Arabian Peninsula, Africa. Therefore, how can ISM be practised in developing countries might differ from Australia.

10.6 Future Research
A number of areas in which future research may be conducted have been identified. These areas are primarily derived from the limitations discussed in the previous section and also the researcher’s identification of research gaps and issues within each ISMP area.

First, in order to address several limitations in this study, similar research into this area should be conducted using multiple case studies with a specific industry (e.g. financial organisations, large organisations and small to medium organisations) to gain an in-depth understanding of how ISMPs are implemented, and identify trends and common approaches within a particular industry.

Second, the study identified the relationship between ISMPs within areas and empirically proved the interdependencies between ISMPs. Future research can be undertaken to investigate how different teams within information security that are responsible for each ISMP area communicate and share required information to improve the quality of the ISMPs in each area.

Third, a possible future extension of this study could be the development of a maturity model of ISMPs for organisations. The ISMP maturity model should include questions related to the ISMPs and different implementation approaches identified in this research that could serve as ISMP maturity criteria to guide evaluators to independently assess their organisation’s as-is
situations. The answers to the questions can be chosen from the maturity attributes that match the organisation’s current ISMPs.

Fourth, in order to achieve generalisation of this study and eliminate the researcher bias, a similar study should be conducted using quantitative methods. Since in-depth understanding and rich insights have been obtained about ISMPs through qualitative exploration, quantitative studies may confirm the findings of this research. In fact, a similar investigation into this area using quantitative studies (e.g. survey), in which ISMPs within areas and related information could be used to develop survey items, may address the generalisability limitations inherent in the scope of this research.

Finally, the researcher has identified several gaps in each ISMP area. There is some possible future research that could be conducted to address the identified gaps. For example, in information security training and awareness (ISTA), future research could explore new approaches that focus not just on providing knowledge about security to the employees, but also on the behavioural and motivational aspects of establishing a security culture. Another example is that measuring the effectiveness of an ISTA program has proved to be very complex, and this needs to be properly investigated. Perhaps future research could conduct in-depth case studies to understand and evaluate the effectiveness of existing ISTA techniques. The last example of future research to address problems identified in ISMP areas is to investigate the organisational challenge of competition for the attention of employees with other training programs that employees have to undertake in the organisation along with the ISTA program.

10.7 Conclusion
The research has sought to answer the research questions concerning the provision of coherent, comprehensive guidance on ISMPs to organisation and ultimately improving the effectiveness of information security management. In doing so, the researcher faced challenges in identifying and addressing the gaps found in the literature and, examining research methods and their suitability to this research. He has understood that being able to make the right research approach choices that are appropriate to the research questions is an important part of being a mature researcher. He has learned about the importance of conducting a review of the literature and synthesis the knowledge around ISMPs to develop the preliminary research framework. In addition, due to the sensitivity of the topic and potential risks that this research might bring to participants, it was also most important to consider ethical approaches to doing research. It made
him realised that ethics was important to gain trust from the participants in order to elicit valuable input from them. He learned how to facilitate the data analysis and to recognise significant findings that emerged from the data. He has experienced the art of reporting, discussing and concluding the findings, and finally crafting these processes a thesis. Through a systematic review of literature, a series of discussions with his supervisors, attending PhD research courses and casual discussions with academics and colleagues, he finally managed to complete his thesis.

This challenging PhD journey has transformed the researcher to become not only a better researcher, but it has transformed him to become a better person. It has revolutionised the way he looks at a problem in life, to fully understand the problem and the potential solutions before attempting to solve it. Thus, it taught him to have the inclination and ability to research on anything, in order to better understand what is going on in the world. Doing a PhD research has improved his communications skills; verbal and written and made his understand about the importance of communicating the knowledge, so others can benefit from it.

In conclusion, this research makes a significant contribution to knowledge and an important contribution to practice through its exploration of how can information security management be practiced in organisation. It provides rich insight about how ISMP areas can should be integrated to constitute an effective ISM. The key contribution of this research is the ISMP framework. The framework provides a holistic and comprehensive guidance for organisations. It represents the first step towards developing a capability maturity model to assist organisations improve the maturity of their information security program.

This research has addressed an identified gap within a multidisciplinary and challenging domain. The research is timely and important substantiated by current level of attention being given to information security issues in mass media.


Björck, F. (2005). *Discovering information security management*. (PhD), Department of Computer and Systems Sciences, Stockholm University,


Hoffman, K.E. (2013). At the ready: incident response has become a more complex art, says Rusty Agee, the city of Charlotte's security leader, 21.


Myers, M.D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and organization, 17(1), (pp. 2-26).


Tan, T., Ruighaver, T., & Ahmad, A. (2003). *Incident Handling: Where the need for planning is often not recognised*. Paper presented at the the 1st Australian Computer, Network & Information Forensics Conference, Perth, Australia (pp. 1-10).


APPENDIX A: RESEARCH METHODOLOGY
DOCUMENTATION

Ethics Approval

29 July 2018

Dr S.B. Maynard
Computing and Information Systems
The University of Melbourne

Dear Dr Maynard,

I am pleased to advise that the Engineering Human Ethics Advisory Group has approved the following project:

Title: Towards a Model of Information Security Management Practices in Organisations

Researchers: Dr A. Ahmad, A/Prof S L Chang, Dr S B Maynard, M Alshalah

Ethics ID: 148319

The Project has been approved for the period: 29-Jul-2015 to 31-Dec-2015.

It is your responsibility to ensure that all people associated with the Project are made aware of what has actually been approved.

Research projects are normally approved for 31 December of the year of approval. Projects may be renewed yearly for up to a total of five years upon receipt of a satisfactory annual report. If a project is to continue beyond five years a new application will normally need to be submitted.

Please note that the following conditions apply to your approval. Failure to abide by these conditions may result in suspension or discontinuation of approval and/or disciplinary action.

(a) Limit of Approval: Approval is limited solely to the research as submitted in your Project application.

(b) Amendments to Project: Any subsequent variations or modifications you might wish to make to the Project must be notified formally to the Human Ethics Advisory Group for further consideration and approval before the revised Project can commence. If the Human Ethics Advisory Group considers that the proposed amendments are significant, you may be required to submit a new application for approval of the revised Project.

(c) Incidents or adverse effects: Researchers must report immediately to the Advisory Group and the relevant Sub-Committee any incidents which might affect the ethical acceptability of the protocol. This includes adverse effects on participants or unforeseen events that might affect continued ethical acceptability of the Project. Failure to do so may result in suspension or cancellation of approval.

(d) Monitoring: All projects are subject to monitoring at any time by the Human Research Ethics Committee.

(e) Annual Report: Please be aware that the Human Research Ethics Committee requires that researchers submit an annual report on each of their projects at the end of the year, or at the conclusion of a project if it continues for less than this time. Failure to submit an annual report will mean that ethics approval will lapse.

(f) Auditing: All projects may be subject to audit by members of the Sub-Committee.

Please quote the ethics registration number and the name of the Project in any future correspondence.

On behalf of the Ethics Committee, I wish you well in your research.

Yours sincerely,

Chair
Engineering Human Ethics Advisory Group
THE UNIVERSITY OF MELBOURNE
DEPARTMENT OF COMPUTING AND INFORMATION SYSTEMS
Research Project Description (Expert Interview)

PROJECT TITLE: Towards a Model of Information Security Management Practices in Organisations

INVESTIGATORS: Moneer Alshaikh
Dr Sean Maynard
Dr Anif Ahmad
Dr Shamion Chang

You are invited to participate in the above research project, which is being conducted by Dr Sean Maynard (Responsible Researcher), Dr Anif Ahmad and Dr Shamion Chang (Co-Researchers), and Moneer Alshaikh (Student Researcher) of the Department of Computing and Information Systems, School of Engineering, The University of Melbourne. This project will form part of Moneer’s PhD research thesis, and has been approved by the School’s Human Ethics Advisory Group (HEAG).

The threat of leakage of trade secrets and intellectual property, disruption of mission-critical systems, and malicious attack from both insiders and outsiders makes information security a high priority for organisations. Although technical security controls have always played a critical role in reducing security risk exposure, recent research has highlighted the critical role of managerial controls in the pursuit of security objectives. Therefore, this research project aims to provide organisations with guidance on the range of practices that can be implemented at part of information security management. To provide comprehensive guidance, this research project develops a model of management-level information security activities.

A comprehensive literature review in the area of information security management has been conducted and led to the development of information security management practices model (ISMPs) that can be implemented to protect organizational information assets. An interview of security experts is planned to be held in order to validate the ISMPs model. The interview is estimated to take about 30 minutes. The first part of the interview aims to understand how an organization manage their information security programs and what are the ISMPs that can be implemented in organisations – from the point of view of the participants. In the second part, the participants would be asked series of questions based on the proposed model of information security management practices in order to validate its elements.

Should you agree to participate in this study, and with your consent, the interview will be audio-recorded in order to ensure that we make an accurate record of what you say. We intend to protect your anonymity and the confidentiality of your responses to the fullest possible extent, within the limits of the law. Your name and contact details will be kept in separate, password-protected computer files from any data that you supply. In the final report, you will be referred to by a pseudonym. We will remove any references to personal information that might allow someone to guess your identity.

Once the thesis arising from this research is completed, a brief summary of the findings will be available for you on request at the Department of Computing and Information Systems. It is also possible that the results will be published in academic journals and/or presented at academic conferences. The data will be kept securely in the Department of Computing and Information Systems for five years from the date of publication, before being destroyed.

Please be advised that your participation in this study is completely voluntary. Should you wish to withdraw at any stage, or to withdraw any unprocessed data you have supplied, you are free to do so without prejudice.

If you require any further information, or have any concerns, please contact the responsible researcher:
Dr Sean Maynard (Responsible Researcher):
Tel: 8344 1573, Email: sean.maynard@unimelb.edu.au

Should you have any concerns about the conduct of the project, you are welcome to contact the Executive Officer, Human Research Ethics, The University of Melbourne, on Tel: 8344 2073, or fax: 8347 6789.
Consent Form

THE UNIVERSITY OF MELBOURNE
DEPARTMENT OF INFORMATION SYSTEMS

Research Project Participant Consent Form (Expert Interviews)

PROJECT TITLE: Towards a Model of Information Security Management Practices in Organisations

INVESTIGATORS: Moneer Alshaikh
Dr. Sean Maynard
Dr. Atif Ahmad
A/Prof Shanton Chang

Name of Participant: ..................................................
Name of Organization: ..................................................

1. I consent to participate in this research project, the details of which have been explained to me, and I have been provided with a written plain language statement to keep.

2. I understand that after I sign and return this consent form it will be retained by the researchers.

3. I understand that my participation will involve an interview which will last for about 60 minutes and I agree that the researcher may use the results as described in the plain language statement.

4. I acknowledge that:
   (a) The possible effects of participating in the interview have been explained to my satisfaction;
   (b) I have been informed that I am free to withdraw from the project at any time without explanation or prejudice and to withdraw any unprocessed data I have provided;
   (c) The project is for the purpose of research only;
   (d) I have been informed that the confidentiality of the information I provide will be safeguarded subject to any legal requirements;
   (e) I have been informed that with my consent the interview will be audio-recorded and I understand that audio-recordings and transcripts will be stored securely at The University of Melbourne and will be destroyed after five years following the last date of publication;
   (f) Any identifying data will be removed and in any publications arising from the work pseudonyms will be used;
   (g) I have been informed that a copy of the research findings will be forwarded to me, should I agree to this.

I consent to this interview being audio-recorded  □ yes □ no
I wish to receive a copy of the summary project report on research findings □ yes □ no

Participant signature: ........................................ Date: ......................

Contact (address / phone number / e-mail / etc.):

..........................................................................................................................

Note: Participant must be over 18 years of age.
**Interview Protocol**

1- Background information
   - What is current role, how long in role, previous roles – how much security experience?
   - What does ISM mean to you?

2- Questions related to ISMPs areas (policy, Risk, ISTA, incident response?)
   - From your experience can you describe the process of policy development in your organisation?
   - Does your security policy link to the organisation’s security requirements?
   - Do you refer to risk assessment to identify what risks need to be addressed by your security policy?
   - Can you describe how risk or incident response informs your organisation security policy?
   - How do you know that your organisation’s security requirements are been met on your security policy?
   - Can you describe the process of writing policy documents? Do you have iterative process of writing, revising and approving the documents before it put to action?
   - In what forms security policy does exist on your organisations? hard copy, soft copy, website … etc.
   - How do you distribute your policy?
   - How does the organisation ensure the policy is being read by employees? (Communicate policy)
   - Can describe how policy is enforced in your organisation?
   - What are the best/ effective strategies for policy enforcement?
   - How can you ensure your policy is relevant and effective?
   - How often do you review your policy?

3- Questions related to IOL
   - In regards to policy management, how often do you talk with other part of organisation as part of your role?
   - Do you spend a lot of time talking to other part of your organisation finance, HR, Marketing, production?
   - What sorts of things do you liaise with other parts of the organisation about?
   - What are your strategies in communicating with other part of the organisation?
   - How do you engage with other people in your organisation?
   - How do you know if your communication with other parts of the organisation has been successful?
APPENDIX B: REPRESENTATIVE EVIDENCE FOR INTERDEPENDENCIES BETWEEN ISMPS

### Risk Management Centred View of Interdependencies

<table>
<thead>
<tr>
<th>#</th>
<th>Interdependencies</th>
<th>Representative Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>The risk assessment report informs the development of IR policy</td>
<td>“part of the planning for incidents is to understand types of risks and their likelihood to be able to prepare for incidence. This information can be found in the risk assessment report” P19_Mng_IR</td>
</tr>
<tr>
<td>R2</td>
<td>The Risk assessment report is required to identify the needs for ISTA program</td>
<td>“There are numerous inputs that go into it. It's, one, understanding the threat landscape: what is currently happening or what's being advertised.” P17_Mng_ISTA</td>
</tr>
<tr>
<td>R3</td>
<td>The Risk assessment report is required to review the ISTA program</td>
<td>“we constantly update our program, create new scenarios and send it to them, change the colour and the look put new cartoon, creates new message out of it because threats keep changing out there. Threats are not the same threats that are here today they will not be here 10 years later”</td>
</tr>
<tr>
<td>R4</td>
<td>The Risk assessment report is required to determine the organisation’s security requirements</td>
<td>“There are a number of ways to do that [identifying requirements]. Often this can be as a result of a risk assessment, because you need to understand what are the key risks to the organisation.” P1_Mng_Policy</td>
</tr>
<tr>
<td>R5</td>
<td>Risk assessment report is required to review the security policy</td>
<td>“If there is a major change in the environment in which you operate, or the system that you operate in that environment, whether procedural or technological, if there is a major change to either of those, you do a risk assessment and see what policies need to be updated.” P4_Mng_Policy</td>
</tr>
<tr>
<td>#</td>
<td>Interdependencies</td>
<td>Representative Evidence</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>R1</td>
<td>Incident response report is required to establish risk management context</td>
<td>“We’d normally take a look at the incident report amongst other things as part of our effort to understand the organisation” P12_Cons_Risk</td>
</tr>
<tr>
<td>R2</td>
<td>Incident response report is required to review risk management process</td>
<td>“Since its incident driven, so basically something significant is happened [incidents] and then someone will go this risk needs to be changed who have the risk going or is may raise that the risk rating needs to change.” P7_Mng_Risk</td>
</tr>
<tr>
<td>R3</td>
<td>The Incident response report is required to identify the needs for ISTA program</td>
<td>“there are numerous inputs that go into it. It's, one, understanding the threat landscape: what is currently happening or what's being advertised” P17_MngISTA “when you find incident for example will be lessons learned from an incident is about how to improve or increase security around an area. Then I think the easiest way to do it is to develop information security awareness. It could be from a slide or as an email that can now be forwarded either to a particular group or to everybody. Depending on who is affected or who benefit from it.” P13_MngISTA</td>
</tr>
<tr>
<td>R4</td>
<td>The Incident response report is required to review the ISTA program</td>
<td>Organisations may also “hire professional consulting organisation and they send fake spam or fishing email or malware to their organisation network it does not impact it but it test how employees react to this test, it is just to check the implementation of SETA program in the organisation.” The aim of such exercise is “to check [whether] (1) the organisation’s system or control detect it or not? (2) what does the users do, click on it or report it? If they are aware of this risk and they have understood they will not click and report it to helpdesk.” P17_MngISTA</td>
</tr>
<tr>
<td>R5</td>
<td>Incident response report is required to determine the organisation’s security requirements</td>
<td>“if it's in a mature organisation, you go through their different risk assessment reports, you go through the change management reports, what happens there? The incidents that have happened, lots of different things.” P3_Cons_Policy</td>
</tr>
<tr>
<td>R6</td>
<td>Incident response report is required to review the security policy</td>
<td>“The policies are often reviewed, but I think it's reviewed as we learn and investigate new incidents. And we apply what's happened in that incident to the policy to make sure the policy is keeping up with what we're seeing in as far as security and the threat landscape. And do we need to add new policy or amend policy to cover those types of events?” P5_Cons_Policy</td>
</tr>
<tr>
<td>#</td>
<td>Interdependencies</td>
<td>Representative Evidence</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>R1</td>
<td>ISTA program is required to communicate the risk assessment results</td>
<td>“Almost every quarter [there are] training and updates. And you need to have somebody that actually can do some sort of analysis and deep dive periodically into the information that’s being prepared to make sure that if things are being misclassified, they’re picked up early and you can go back and rectify that either through additional training or clarification.” P9_Mng_Risk</td>
</tr>
<tr>
<td>R2</td>
<td>ISTA program is required to prepare for incidents</td>
<td>“When you are faced with an incident that has the potential to be major, you need to have the procedures very clear and very rehearsed, and the people need to be well trained on their roles and responsibilities, and how everybody fits in that team.” P22_Mng_IR</td>
</tr>
<tr>
<td>R3</td>
<td>ISTA program is required to communicate the security policy</td>
<td>“The best way [to communicate security policy] is to develop an internal portal [computer based training] CBT where the organisation can ensure that its employees have read and signed that policy.” P2_Cons_Policy \ “There are multiple ways of doing it [communicating policy]. We were doing it through awareness campaign.” P3_Cons_Policy</td>
</tr>
<tr>
<td>R4</td>
<td>ISTA program is required to enforce the security policy</td>
<td>“One of the ways to enforce policy is to provide mandatory training. This is regarded as one of the ways of enforcement” P5_Cons_Policy.</td>
</tr>
<tr>
<td>R5</td>
<td>The development of security policy is required for ISTA program</td>
<td>“first you need to have a policy because it is policy that you need your employees to be aware of” P13_Mng_ISTA</td>
</tr>
</tbody>
</table>
Author/s: Alshaikh, Moneer

Title: Information security management practices in organisations

Date: 2018

Persistent Link: http://hdl.handle.net/11343/208934

File Description: Information security management practices in organisations

Terms and Conditions: Copyright in works deposited in Minerva Access is retained by the copyright owner. The work may not be altered without permission from the copyright owner. Readers may only download, print and save electronic copies of whole works for their own personal non-commercial use. Any use that exceeds these limits requires permission from the copyright owner. Attribution is essential when quoting or paraphrasing from these works.