TOP MANAGEMENT ENGAGEMENT IN INFORMATION SECURITY: MULTIPLE-CASE STUDIES OF MALAYSIAN PUBLIC SECTOR

BY

RUFIZAH ABDUL MUNIR

A thesis submitted in fulfillment of the requirement for the degree of Doctor of Philosophy of Information Technology

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

FEBRUARY 2024

ABSTRACT

Organisations that rely heavily on ICT face greater challenges in protecting their information assets. Technical solutions alone cannot guarantee the security of an organisation's information. As human is the weakest link, numerous studies on information security now incorporate human factors as part of the information security solution. As security is integral to corporate governance, top-level commitment and management roles are indispensable to forming good information security governance (ISG). Through this governance, the sustainability of information security activities in organisations could be achieved. However, due to top management's common perception of information security as a technical and operational concern rather than a business matter, the responsibility for its implementation is often assigned solely to the information security team. This approach has led to challenges in fostering a collaborative, organisation-wide effort towards information security. Therefore, this study aims to gain clarity on the phenomenon of top management driving information security initiatives in the Malaysian government. It will examine the factors that influence their engagement in information security and seek to explore the issues related to ISG. This study employs qualitative research methodology with an inductive approach. The multiple-case study is used as a strategy to investigate the topic under study. Using purposive sampling, interviews were conducted at four (4) public sector organisations involving 27 participants. The results indicate that Regulatory Forces (External Factor), Informal Education (Personal Factor), and On-the-job Exposure (Personal Factor) are the most influential factors on top management engagement in information security. The application of the information security engagement factors led to the establishment of the research model of the study. This study proposes the extension of Malaysia's cyber security framework (RAKKSSA) and its accompanying guidelines to demonstrate the research model's viability. The extension focuses on top management competency, an area where the current RAKKSSA is deficient. The extended RAKKSSA improves the overall comprehensiveness of the framework. It guides all levels of government agency personnel with the essential skillsets, from governing information security initiatives to carrying out security activities within their respective organisations.

ملخص البحث

تواجه المؤسسات التي تعتمد بشكل كبير على تكنولوجيا المعلومات والاتصال (ICT) تحديات متزايدة في حماية أصول معلوماتها. ولا يمكن للحلول التقنية وحدها ان تضمن أمن معلومات المؤسسة إذ يعتبر العامل البشري الحلقةَ الأضعف، لهذا تقوم العديد من الدراسات حول أمن المعلومات بدمج العواملَ البشرية كجزء من حلول أمن المعلومات. وبما أن الأمن يعتبر جزءً أساسياً من حوكمة الشركات، فلا يمكن الاستغناء عن التزام الإدارة العليا والمناصب الإدارية في تشكيل حوكمة جيدة لأمن المعلومات (ISG) من خلال هذه الحوكمة، يمكن تحقيق استدامة لأنشطة أمن المعلومات في المؤسسات. ومع ذلك، نظراً لتصور الإدارة العليا الشائع للأمن المعلوماتي كمشكلة تقنية وتشغيلية بدلاً من مسألة تجارية، يتم تحميل المسؤولية عن تنفيذها عادةً إلى فريق أمن المعلومات وحده. وقد أدى هذا النهج إلى تحديات في تبني جهد تعاوني على مستوى المؤسسة تجاه أمن المعلومات. لذا، يهدف هذا البحث إلى توضيح ظاهرة قيادة الإدارة العليا لمبادرات أمن المعلومات في حكومة ماليزيا. سيقوم البحث بفحص العوامل التي تؤثر في مشاركتهم في أمن المعلومات وسيسعى إلى استكشاف القضايا المتعلقة بحوكمة أمن المعلومات. يستخدم هذا البحث منهجية البحث النوعي مع نهج استقرائي. ويستخدم حالات متعددة كاستراتيجية للتحقيق في الموضوع المدروس. باستخدام عينات هادفة، تم إجراء مقابلات في أربع منظمات في القطاع العام تشمل 27 مشاركاً. تشير النتائج إلى أن القوى التنظيمية (عامل خارجي)، والتعليم غير الرسمي (عامل شخصي)، والتعرض في العمل (عامل شخصي) هي العوامل الأكثر تأثيراً في مشاركة الإدارة العليا في أمن المعلومات. وأدى استخدام عوامل مشاركة أمن المعلومات إلى إنشاء النموذج المقترح من قبل هذا البحث. حيث برهنت الإضافة المقترحة لإطار الأمن السيبراني في ماليزيا (RAKKSSA) ودليل الإرشادات المرافق لها على جدوى النموذج. تركز الإضافة على كفاءة الإدارة العليا، وهي جزئية تعاني من النقص في نسخة RAKKSSA الحالية. فمن خلال دمج مكون كفاءة الإدارة العليا والإرشادات في الإضافة المقترحة، يصبح RAKKSSA إطاراً شاملاً، فيغطي الإرشادات من البداية إلى النهاية لجميع القطاعات العامة الماليزية لتطوير سياسات أمن المعلومات وتنفيذ مبادرات الأمن في مؤسساتها.

APPROVAL PAGE

The thesis of Rufizah Abdul Munir has been approved by the following:

_____
Shuhaili Talib
Supervisor

_____
Nurul Nuha Abdul Molok
Co-supervisor

_____
Akram M Z M Khedher
Internal Examiner

_____
Azah Anir Norman
External Examiner

_____
Mohamed Elwathig Saeed Mirghani
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Rufizah Abdul Munir

Signature…… Date…19 February 2024…

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

TOP MANAGEMENT ENGAGEMENT IN INFORMATION SECURITY: MULTIPLE-CASE STUDIES OF MALAYSIAN PUBLIC SECTOR

I declare that the copyright holder of this thesis is International Islamic University Malaysia.

Affirmed by Rufizah Abdul Munir

…… 19 February 2024

Signature Date

This thesis is dedicated to the people that mean the world to me

My late mother, father, and husband

I am truly grateful for the profound influence you have had on shaping who I am today

Thank you for making it possible

ACKNOWLEDGEMENTS

Allah, the Almighty, whose Grace and Mercies have been with me throughout my doctoral studies, deserves all praise. His Mercies and Blessings on me eased the herculean task of completing this thesis, despite its difficulty.

Assistant Professor Dr Shuhaili Talib and Assistant Professor Dr Nurul Nuha Abdul Molok, whose enduring disposition, kindness, promptness, thoroughness, and friendship facilitated the successful completion of my study, are most deserving of my gratitude. I would like to acknowledge and thank them for their insightful comments, suggestions, and questions, which significantly improved the research. In addition, their exceptional understanding of this study's purpose and subject matter resulted in insightful feedback that greatly assisted me. Furthermore, despite their obligations, they took the time to listen and help me whenever I asked. Without a doubt, the moral support they provided aided me in constructing and writing the thesis.

I am also grateful to my supervisory committee and its chairman, Professor Ts Dr Abdul Rahman Ahlan, whose assistance and cooperation contributed to the success of this research. Professor Dr Atif Ahmad and Associate Professor Dr Sean Maynard, my supervisors during my time as an Academic Visitor at the University of Melbourne, Australia, also deserve my appreciation. Thank you for your guidance during my time as an Academic Visitor at the institution. I had such a good time in Melbourne!

Lastly, I would like to extend my heartfelt gratitude to the translator, Muhammad Alfatih Muddathir who diligently attended to my needs. I am also deeply thankful to everyone who prayed for me, was patient with me, understood my situation, and helped me along the way—my sister, family, relatives, research mates, best friends, bosses, colleagues, and all well-wishers. Sincere thanks!

Again, I glorify Allah for His inexhaustible mercy on me, one of which is allowing me to complete the PhD journey successfully. Alhamdulillah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATION

APT	Advance Persistent Threat
BPM	Information Management Division
CEO	Chief Executive Officer
CGSO	Chief Government Security Officer
CIA	Confidentiality, Availability and Integrity
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNII	Critical National Information Infrastructure
CSM	Cyber Security Malaysia
DKICT	ICT Security Policy
DRC	Disaster Recovery Center
E	External
ERP	Enterprise Resource Planning
F	Information System (Scheme)
GCert	Government Computer Emergency Response Team
GST	Goods and Services Tax
HQ	Headquarters
HRMIS	Human Resources Management System
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IIUM	International Islamic University Malaysia
IS	Information Security
ISG	Information Security Governance
ISM	Information Security Management
ISMS	Information Security Management Systems
ISO/IEC	International Organisation for Standardization/International Electrotechnical Commission
ICTSO	Information and Communication Technology Security Officer
ISP	Information Security Strategic Plan
ISS	Information Systems Security
IT	Information Technology
ITG	Information Technology Governance
JPA	Public Service Department Malaysia
JPICT	ICT Steering Committee
KBS	Ministry of Youth and Sports
KDN	Ministry of Home Affairs
KKMM	Ministry of Communications and Multimedia
KP	Director General
KPI	Key Performance Indicator
KSN	Chief Secretary

KSU	Secretary General
M	Administrative and Diplomatic (Scheme)
MAMPU	Malaysian Administrative Modernization and Management Planning Unit
MCMC	Malaysian Communications and Multimedia Commission
MCO	Movement Control Order
MCSS	Malaysian Cyber Security Strategy
MinDef	Ministry of Defence
MKN	National Security Council
MPC	Multiple Perspective Concept
MPT	Top Management Meeting
MS	Malaysia Standard
MSC	Multimedia Super Corridor
MyGPI	Malaysian Government Performance Index
NACSA	National Cyber Security Agency
NCSP	National Cyber Security Policy
NC4	National Cyber Control and Coordination Center
NIS	Non-Information Security
NIT	Neo-Institutional Theory
PKP	Business Continuity Plan
PMO	Prime Minister's Office
PTD	Administrative and Diplomatic Officer
QAS	Quality Assurance Services
RAKKSSA	Public Sector's Cyber Security Framework
RO	Research Objective
RQ	Research Question
SETA	Security, Education, Training and Awareness
SIRIM	Standards and Industrial Research Institute of Malaysia
SME	Small and Medium Enterprises
SOP	Standard Operating Procedure
SPA	Security Posture Assessment
SPSS	Statistical Package for the Social Sciences
SSR	System Star Rating
SUB	Undersecretary
TKP	Deputy Director General
TKSU	Deputy Secretary General
TM	Top Management
TOP	Technical, Organisational, Personal
TOR	Terms of Reference

CHAPTER ONE

INTRODUCTION

1.1 OVERVIEW

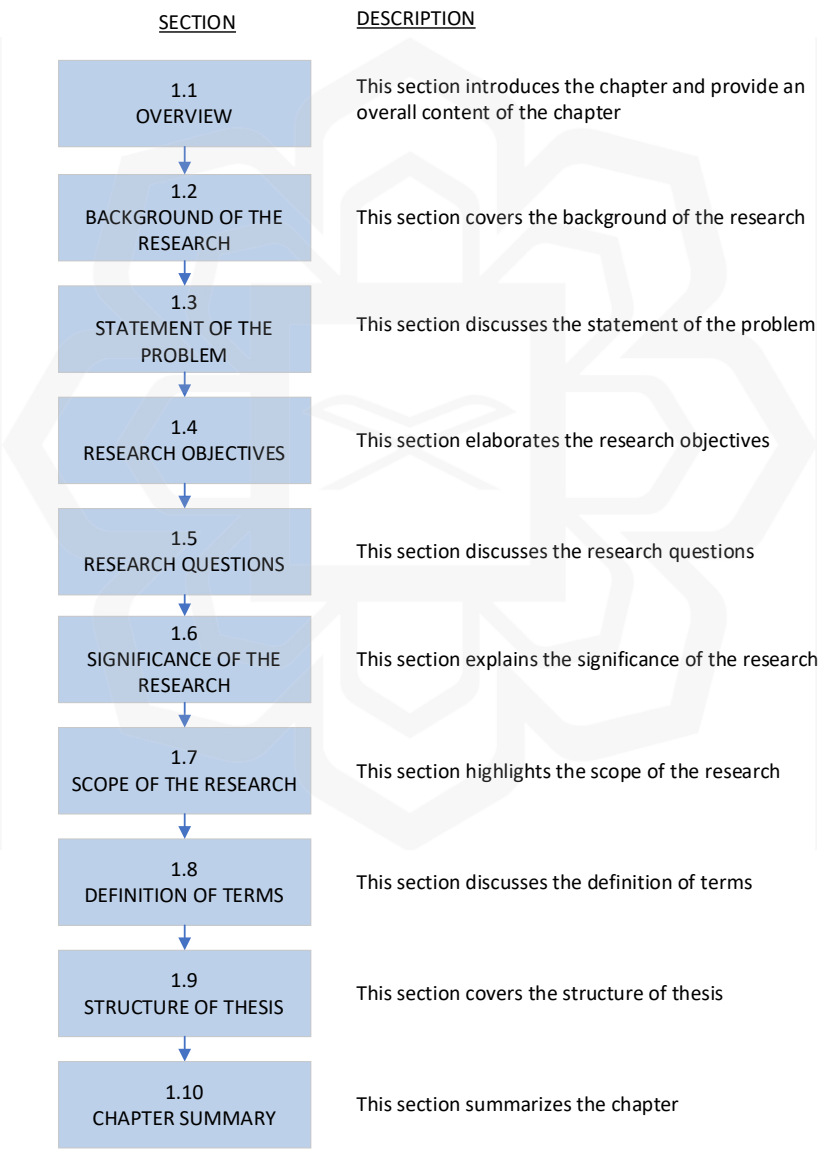
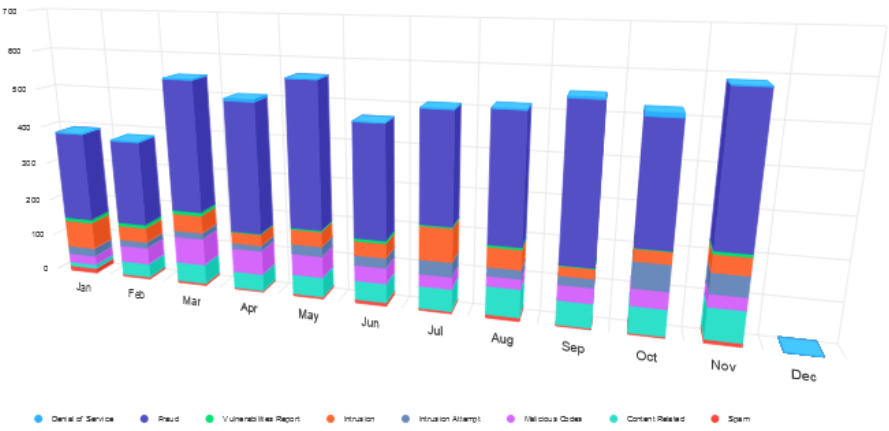


Figure 1.1: Organisation of Chapter One

1.2 BACKGROUND OF THE RESEARCH

In today's world, computers are more interconnected than ever before and are being used extensively in organisations. The dependency on computers, and information and communication technology (ICT) in running overall business operations, which include technology, people and process elements, could expose organisations to cyberthreats and information security risks (Lee, 2021; Posthumus & Von Solms, 2004; Razali & Said, 2015) and exert influence on the financial and reputational consequences (Boitan, 2019). Despite efforts that have been made to mitigate information security risks and threats, substantial volumes of computer breaches and cybercrimes remain significantly high (Lee, 2021; Ula et al., 2011). An IBM analysis revealed that the average cost of a data breach surged to almost US$4.5 million in 2023 (Ernst & Young, 2023a). Meanwhile, in a recent report by CyberSecurity Malaysia (2023), the total number of reported incidents between January and October 2023 is 4,898, as illustrated in Figure 1.2.



#	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Denial of Service	0	1	2	4	0	1	1	2	4	8	2	0	25
Fraud	235	222	340	338	374	290	279	322	388	299	360	0	3,447
Vulnerabilities Report	10	9	9	2	3	7	5	6	2	2	8	0	63
Intrusion	72	39	46	30	39	37	84	49	23	29	43	0	491
Intrusion Attempt	22	17	17	15	26	27	38	23	23	66	49	0	323
Malicious Codes	24	45	71	62	57	41	32	27	38	43	32	0	472
Content Related	12	37	53	45	51	50	58	72	62	66	79	0	585
Spam	13	6	5	4	6	9	5	9	4	4	9	0	74
	388	376	543	500	556	462	502	510	544	517	582	0	5,480

Figure 1.2: Reported incidents based on general incident classification statistics 2023 (CyberSecurity Malaysia, 2023)

Based on the statistics, incidents involving fraud, content related, intrusion, malicious code, and intrusion attempt remained high for 12 consecutive months. Even though the figures for other threats are lesser, they must be addressed appropriately. As a result, organisations which rely heavily on ICT to operate their business have taken information security seriously and started to increase their investment in building more secure virtual business environments. The global poll of 500 cybersecurity leaders by Ernst & Young (2023) reveals increasing expenses linked to cybersecurity expenditure and an average of 44 cyber incidents occurring in 2022. Chief Information Security Officer (CISO)

respondents indicate that they spend an average of US$35 million per year on cybersecurity. They also note that the typical cost of a breach to their organisation has risen by 12% to US$2.5 million in 2023 and is expected to reach US$4 million. Once the global cyber-attack called theWannaCry ransomware, affecting thousands of computers in more than 100 countries worldwide is a harsh reminder for every organisation to protect their sensitive and confidential information aggressively. Therefore, it can be concluded that there will always be a need to increase funding to combat security threats and crimes.

Unfortunately, many organisations' funding and efforts are directed and focused only on technical components. According to Von Solms (2006), until the early 1980s, solutions to information security primarily focused on technical issues. However, experts have now realized that technological solutions alone could not guarantee secure mechanisms for organisational information (Khando et al., 2021; Safa et al., 2015; Tsohou et al., 2008). In fact, 100% security of information is impossible because all possible risks, threats and vulnerabilities are never known (Khando et al., 2021; Singh et al., 2013). They grow and evolve due to technological advancement in the ICT world. Information security issues need to be tackled from a broader, holistic approach to preserving the confidentiality, integrity and availability (CIA) of the information. For that reason, many studies in information security have started to incorporate the human aspects as well as managerial aspects and are no longer limited to technology issues (Karlsson et al., 2015; Khando et al., 2021; Silic & Back, 2014; Siponen & Oinas-Kukkonen, 2007; Soomro et al., 2016; Tsohou et al., 2008). This includes the governance component, where the top management has a vital role in establishing and managing information security in organisations (AlGhamdi et al., 2020; Soomro et al., 2016; Von Solms, 2001) to handle business and IT risks (Singh et al., 2013). Commitment and managerial roles from the top management are crucial not only to guarantee security initiatives can be implemented throughout the organisations, but also to ensure sustainability and continuous maintenance of information security activities within the organisations.

1.3 STATEMENT OF THE PROBLEM

In a study of the user involvement concept by Barki & Hartwick (1989), top management support positively influences employees' attitudes and behaviour in information systems implementation. Similarly, in the context of information security, active commitment from top management to information security initiatives could motivate employees to comply with the information security standards and policies in organisations. Top management's responsibility is to develop functional governance and implementation of information security to preserve the CIA of information assets. Without proper governance of information security initiatives, information assets could easily be exposed to various risks, compromising information and reducing its value (Gantz & Philpott, 2013; Whitman & Mattord, 2012a). However, there is a glaring issue in the Malaysian government where *information security practices are challenging to implement and appreciate throughout the organisation.*

One of the problems behind this issue is that *the implementation of information security is often delegated to technical people from the IT unit* (Gale et al., 2022; Whitman & Mattord, 2012a). They are tasked to shape the security behaviour throughout the organisations with minimal or no support from the top management. According to Kim & Kim (2015) and Singh & Gupta (2019), organisation-wide information security initiatives face numerous challenges and appear to receive insufficient support from top management. Most notably, information security programs are not adequately supported by a committee consisting of top management (Kim & Kim, 2015; Singh & Gupta, 2019). This leads to another problem: top management's minimal commitment to driving information security in their organisations.

Another problem, as argued by previous studies, is that *top management's engagement in information security initiatives is relatively low* (Chang & Ho, 2006a; Gale et al., 2022; Hsu, 2009; Hu et al., 2007b). Several studies (Barton, 2014; Hu et al., 2007b; Liang et al., 2007a) have identified that external pressures affect top management involvement. On the other hand, according to a study by Abdul Molok et al. (2013), a lack

of commitment by the top management might be related to management's perception, commitment, and responsibility.

There is also a problem when *information security initiatives are handled as a one-time project instead of a continuous process and improvement.* When this occurs, it is not easy to sustain and maintain information security initiatives in the long run. Although there is a substantial amount of literature on security in general, there is a scarcity of study specifically focused on security governance (Nicho, 2018) in the government sector and the level of commitment from top management in information security (Gale et al., 2022). There is a lack of comprehensive field investigations that aim to examine the issues surrounding the involvement of top management in information security within public sector organisations. Nevertheless, this gap does not arise from a lack of appeal in the field of information security governance studies. In fact, every organisation requires support from top management to implement information security as their commitments have the most significant impact on the success or failure of an information security project initiative (Young & Jordan, 2008). Given the limited literature on top management engagement's perspective of information security in government sector, this study attempts to explore the phenomena using a case study methodology and develop a comprehensive list of the influential factors. Therefore, this research would provide a deeper understanding of the top management's issues and problems in information security governance. Filling this gap will make a valuable contribution to the body of knowledge.

1.4 RESEARCH OBJECTIVES

This research aims to study top management engagement in governing information security initiatives in Malaysian public sector organisations. The following are the Research Objectives (RO) that this study aims to achieve:

> ***Primary RO:*** *To understand how can top management engagement in information security be improved in Malaysian public sector organisations.*

RO1: *To investigate how top management drives information security initiatives within Malaysian public sector organisations;*

RO2: *To determine the factors influencing top management engagement in information security governance;*

- ***RO2.1:*** *To identify the determinants that influence top management engagement in information security*
- ***RO2.2:*** *To develop a research model based on the factors identified in RO2.1*
- ***RO2.3:*** *To establish an extension of Malaysia's Cyber Security Framework (RAKKSSA) document and its accompanying guidelines based on the engagement factors*

RO3: *To explore the issues related to top management governing information security initiatives in their organisations.*

1.5 RESEARCH QUESTIONS

Research questions (RQ) are formulated to answer the research objectives specified in the previous section. Listed below are the three (3) RQs that this study seeks to address:

Primary RQ: *How can top management engagement in information security be improved in Malaysian public sector organisations?*

RQ1: *How does top management govern information security in organisations?*

RQ2: *What are the factors influencing top management engagement in organisations?*

RQ3: *What are the issues faced by the top management in governing information security in their organisation?*

These research questions impact most other steps taken to perform the study. The researcher constructs interview questions based on the research questions to gather the information needed to understand and further meet the study's objectives.

Interview questions are designed to be flexible, allowing the same questions to be posed to three (3) different groups of respondents. Interestingly, this enables answers to the same questions to be seen through *different viewpoints* or *multiple perspectives*. Since the study focuses primarily on top management engagement in information security governance; thus, the first perspective concerns top management, such as CIOs. They become the primary respondents in providing input to meet the research questions. The next perspective comes from the respondents who work in information security in their respective organisations. The final perspective comprises respondents who are not involved in information security and are attached to various departments in the organisation.

1.6 SIGNIFICANCE OF THE RESEARCH

The findings of this study can be applied as a foundation for further research on information security governance, particularly in regard to the engagement shown by top management and their level of commitment. The following is a list of the contributions that the proposed research will make:

(a) Theoretical Implications

i. Allows researchers and practitioners, particularly in the public sector, to comprehend the factors that contribute to the involvement of top management in information security initiatives.

ii. Extends the use of theories and models, specifically the Multiple Perspectives Concept and the Neo-Institutional Theory, in the context of top management and their engagement in security issues.

(b) Methodological Implications

i. Development of the initial research model to study the multiple perspectives of the factors influencing top management engagement, which can be used to aid in the collection of data for the case studies.

ii. Aids in the analysis of the case study results.

(c) Practical Implications

i. Provides organisations and the information security community with a broader understanding of top management participation in information security, which leads to more effective security governance.
ii. Allows organisations to design or improve their current information security competency development programs for top management through personalised training and awareness programs.
iii. Assists top management in comprehending their roles and responsibilities in information security initiatives within their respective organisations.

1.7 SCOPE OF THE RESEARCH

The Malaysian government has made numerous efforts to safeguard vital information infrastructures. Establishing the National Cyber Security Policy (NCSP) in 2006 was one of the efforts. Due to the reliance on ICT infrastructures, this policy is designed to deal with dynamic cyber threats (CNII Portal, n.d.). NCSP aims to address the current and future cyber risks faced by Critical National Information Infrastructure (CNII) sectors as follows:

- National Defence and Security
- Banking and Finance
- Information and Communications
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency Services
- Food and Agriculture

It is intriguing to investigate how public sector organisations view government-led information security initiatives. In addition, it is essential to investigate how organisations

in the public sector implement information security in accordance with national and government information security policies. This research is conducted within public sector organisations for these reasons.

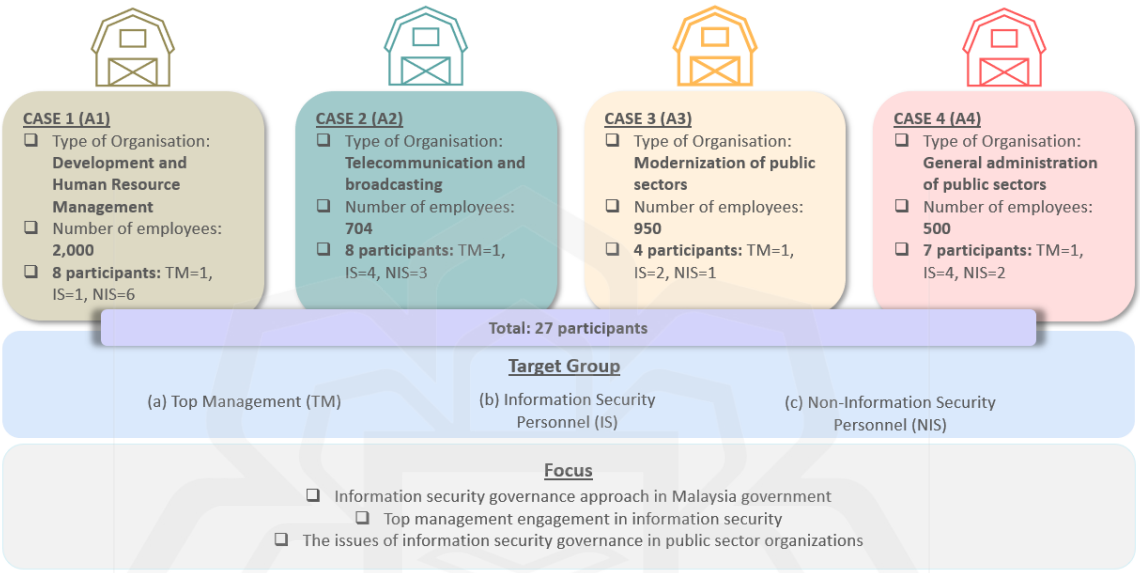


Figure 1.3: Research scope

According to Figure 1.3, this research focuses on the scope as follows:

(a) The target organisations are the public sector organisations in Malaysia. The ministries and agencies are selected based on the differences in their core services (4 organisations).

(b) The target group comprises top management, information security personnel, and personnel indirectly involved in information security work (27 participants).

(c) The focus of the study revolves around information security governance and practices, the engagement of top management in information security, and the issues revolve around information security within Malaysian public sector organisations.

1.8 DEFINITION OF TERMS

Information Security Governance (ISG)

A set of guidelines related to information security instructs top management on how to create and maintain control environments, as well as the processes and systems that facilitate their operation. It provides information security strategic direction, ensures that objectives are met, effectively manages risks, makes efficient use of organisational resources, and evaluates the enterprise security program's success or failure. It also indicates the extent to which top management and other administrations are engaged in information security within an organisation (IT Governance Institute, 2006; Moulton & Coles, 2003; Posthumus & Von Solms, 2004; Sajko et al., 2011).

Top Management

An individual or group that directs and controls an organisation at its highest level (Von Solms & Von Solms, 2009). The executive leadership has the authority to delegate authority and allocate resources within the organisation. This study's target audience consists of high-ranking officers in public sector organisations who are actively involved in information security committees/groups, such as the Chief Information Officer (CIO). The mapping of top management in the Malaysian public sector with the ISG Framework by Posthumus & Von Solms (2004) is illustrated in Table 2.3 (Chapter Two).

Information Security Personnel (IS)

An employee who is attached to an organisation's information security team. Their responsibility includes managing security incidents. In addition, they may be involved in planning and implementing preventative security measures and developing disaster recovery plans.

Non-Information Security Personnel (NIS)

An employee of an organisation who is not an Information Security Personnel.

Engagement

Engaging with a person or thing in order to gain a better understanding of that thing or person (Cambridge Dictionary, n.d.) (see Section 2.4.1).

1.9 STRUCTURE OF THE THESIS

This thesis is comprised of six (6) sections, and each chapter is interrelated. The chapters are meant to be read as a whole. The first three (3) chapters of the thesis provide an overview of the research topic, a discussion of relevant literature, and an outline for carrying out the research. The study's field investigation and general analysis and summary are described in Chapter Four, Five, and Six. The sequence and linkages between sections in each chapter are represented in the research alignment matrix in Table 1.1.

Table 1.1: Research alignment matrix

CHAPTER ONE				CHAPTER FOUR	CHAPTER FIVE	CHAPTER SIX
Issue	**Problem Statement**	**Research Objective (RO)**	**Research Question (RQ)**	**Data Analysis and Research Findings**	**Discussion**	**Conclusion**
Information security practices are challenging to implement and appreciate throughout the organisation.		**Primary RO:** To understand how can top management engagement in information security be improved in Malaysian public sector organisations	**Primary RQ:** How can top management engagement in information security be improved in Malaysian public sector organisations?			
	Sub-problem 1: Information	**RO1:**	**RQ1:**	**Section 4.3.1** Theme 1:	**Section 5.2** Information	**Section 6.2.1**

CHAPTER ONE				CHAPTER FOUR	CHAPTER FIVE	CHAPTER SIX
Issue	**Problem Statement**	**Research Objective (RO)**	**Research Question (RQ)**	**Data Analysis and Research Findings**	**Discussion**	**Conclusion**
	security matters delegated to the information security team *(How is the current implementation?)*	To investigate how top management drives information security initiatives within Malaysian public sector organisations.	How does top management govern information security in organisations?	Information Security Governance Approach	Security Governance Approach	Information Security Governance Approach
	Sub-problem 2: Engagement from the top management is low	**RO2:** To determine the factors influencing top management	**RQ2:** What are the factors influencing top management	**Section 4.3.2** Theme 2: Factors Influencing Top Management	**Section 5.3** Factors Influencing Top Management Engagement in	**Section 6.2.2** Factors Influencing Top Management Engagement

CHAPTER ONE				CHAPTER FOUR	CHAPTER FIVE	CHAPTER SIX
Issue	**Problem Statement**	**Research Objective (RO)**	**Research Question (RQ)**	**Data Analysis and Research Findings**	**Discussion**	**Conclusion**
	(What are the factors affecting their engagement?)	engagement in information security governance. **RO2.1:** To identify the determinants that influence top management engagement in information security	engagement in organisations?	Engagement in Information Security	Information Security	**Section 6.3** Revised Model of the Study **Section 6.4** The Extension of RAKKSSA's Competency Guidelines

CHAPTER ONE				CHAPTER FOUR	CHAPTER FIVE	CHAPTER SIX
Issue	**Problem Statement**	**Research Objective (RO)**	**Research Question (RQ)**	**Data Analysis and Research Findings**	**Discussion**	**Conclusion**
		RO2.2: To develop a research model based on the factors identified in RO2.1 **RO2.3:** To establish an extension of Malaysia's Cyber Security Framework (RAKKSSA) document and				

CHAPTER ONE				CHAPTER FOUR	CHAPTER FIVE	CHAPTER SIX
Issue	**Problem Statement**	**Research Objective (RO)**	**Research Question (RQ)**	**Data Analysis and Research Findings**	**Discussion**	**Conclusion**
		its accompanying guidelines based on the engagement factors				
	Sub-problem 3: Information security initiatives are treated as a one-off project rather than a continual process	**RO3:** To explore the issues related to top management governing information security initiatives in	**RQ3:** What are the issues faced by the top management in governing information security in their organisation?	**Section 4.3.3** Theme 3: Information Security Governance Issues	**Section 5.4** Information Security Governance Issues	**Section 6.2.3** Issue in Information Security Governance

CHAPTER ONE				CHAPTER FOUR	CHAPTER FIVE	CHAPTER SIX
Issue	**Problem Statement**	**Research Objective (RO)**	**Research Question (RQ)**	**Data Analysis and Research Findings**	**Discussion**	**Conclusion**
	(What are the issues revolved around information security governance?)	their organisations.				

1.10 CHAPTER SUMMARY

This chapter provides in detail the background of the research (Section 1.2), which lead to the discussion of the problem statement (Section 1.3), followed by the list of research objectives (Section 1.4) and research questions (Section 1.5). This chapter also covers the significance of this study (Section 1.6) and its scope (Section 1.7). The definition of important terms used in this study is also highlighted (Section 1.8). The last part is the thesis structure which illustrates the sequence and linkages of sections in each chapter (Section 1.9).

CHAPTER TWO

LITERATURE REVIEW

2.1 OVERVIEW

Figure 2.1 presents the overview of how this literature review chapter is organised. Generally, Chapter 2 is divided into two (2) parts. Part One consists of the literature on information security until a review of information security initiatives and implementation in Malaysian public sector organisations. Part Two, on the other hand, covers the theoretical background which contributes to the development of the initial research model of this study. Part One and Part Two organisations are explained in Section 2.2 and Section 2.8, respectively.

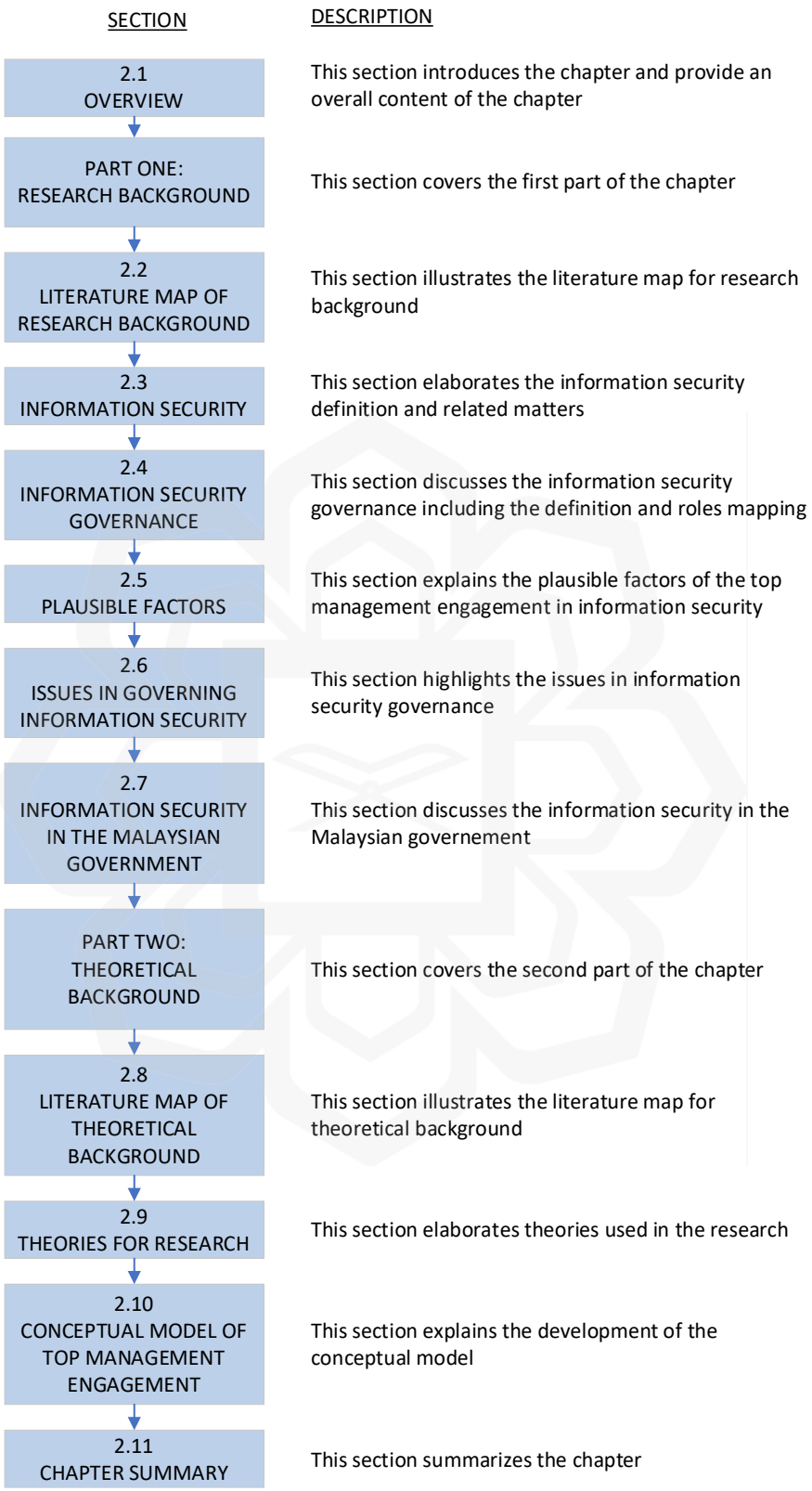


Figure 2.1: Organisation of Chapter Two

Completing a literature review improves a researcher's ability to comprehend and perform a study on a given topic. In point of fact, it serves as the basis for carrying out the study by investigating past research and the present issues associated with the work that must be done in the future. In addition, it assists the researcher in constructing the research model based on the theories, earlier models, and previously conducted investigations. As a result, this chapter's purpose is to review the relevant literature to provide the researcher with the tools necessary to identify the gaps in the existing research and define appropriate terminology concerning the research questions and objectives. The following section goes into detail about the literature review for this study.

PART ONE: R ESEARCH BACKGROUND

2.2 LITERATURE MAP OF RESEARCH BACKGROUND

Figure 2.2 shows Part One of this chapter, which covers the whole scope of information security topics. Later on, the literature focused on information security governance to understand the notion of information security governance and why the role of top management in managing information security inside an organisation is so critically important. The determinants that are found to influence the engagement of top management are then collated when they have been discovered. In addition to the factors to be considered, all issues pertaining to information security will be presented. Then, studies on the information security measures taken by government agencies in Malaysia are being carried out to gain an understanding of how information security functions, the agencies responsible for acting as a centre and consultant on information security, and what initiatives the government has put into place to address information security-related issues. The researcher can carry on with the research of top management engagement in public sector organisations and accommodate any more findings to fulfil the research objectives.

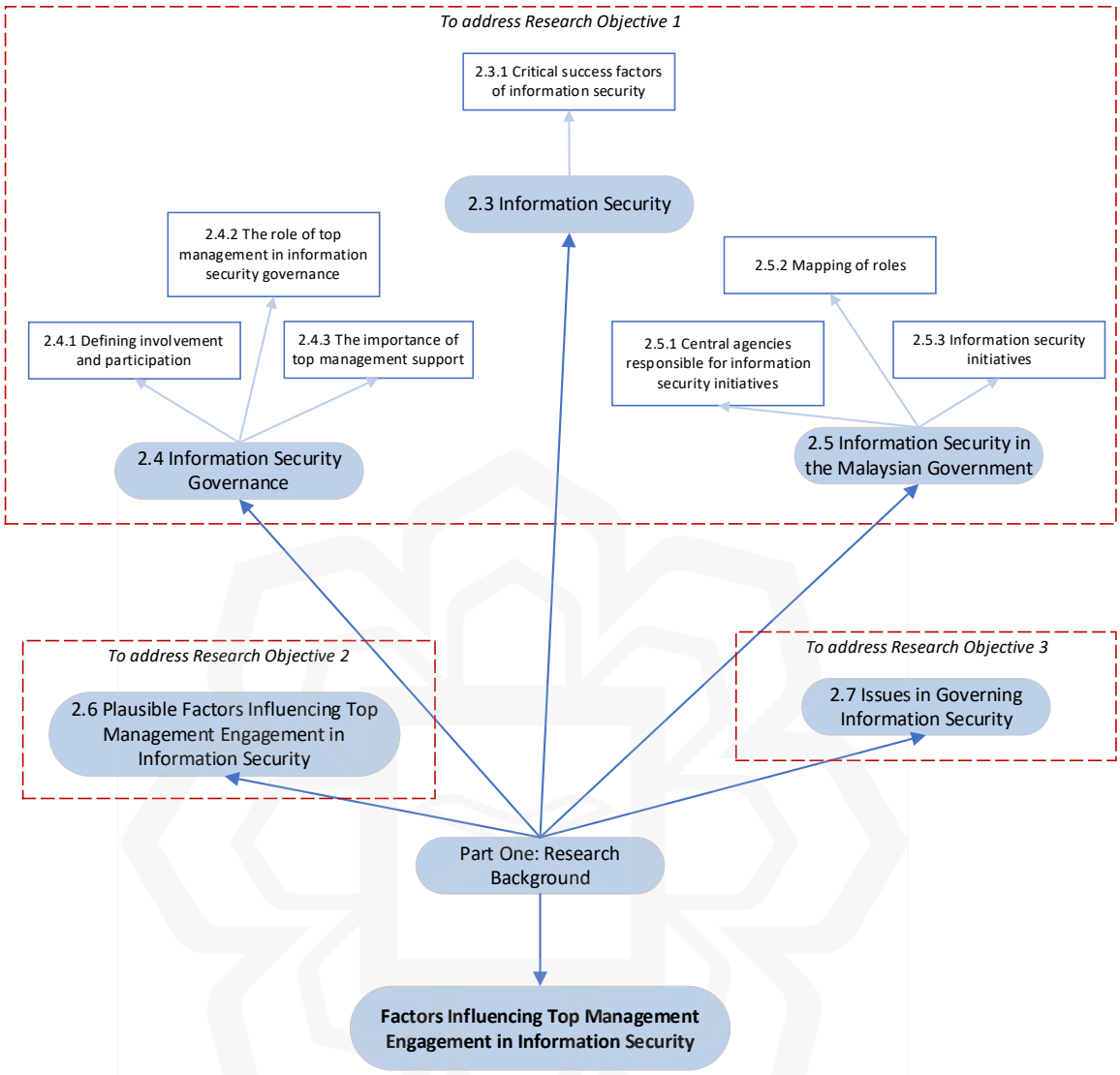


Figure 2.2: Literature map of research background

2.3 INFORMATION SECURITY

As described in ISO/IEC 27000, information is "an asset that, like other important business assets, is essential to an organisation's business and consequently needs to be suitably protected" (International Standard ISO/IEC 27000, 2018, p.12). Meanwhile, IEEE Standard Computer Dictionary defined information as "the meaning that humans assign to data by means of known conventions that are applied to the data" (IEEE Computer Society, 1990). According to ISO/IEC 27000, there are many ways for information to be stored –

digital and material. Knowledge held by employees is also considered as information, which is called "unrepresented information" (International Organisation for Standardization, n.d.-a). According to Ahmad et al. (2005), data can also be saved on cognitive media, such as the minds of individuals. Due to the fact that information can have varying degrees of sensitivity, it can be hard to keep under wraps, and leaks can occur (Ahmad et al., 2005). From the definition of information, it can be seen that information is considered to be unstructured and can exist in a number of different ways, including being written down on paper, saved on computers, delivered via mail or electronically, presented on film, articulated in conversation (Von Solms & Niekerk, 2013), or even in a person's mind (Ahmad et al., 2005).

Consequently, based on these definitions, this study defines information as a valuable asset for organisations that require proper protection against all types of threats and risks, regardless of the storage and transmission medium. The protection includes the process by which data is recorded, processed, shared, retrieved, and destructed information from electronic mediums (Williams, 2001a).

The definitions of information also extend the meaning of information security which relates to the protection of information against loss, improper disclosure or damage. According to ISO/IEC 27000, information security is defined as the *"preservation of confidentiality, integrity and availability of information"* (SIRIM QAS International, n.d.). Von Solms & Von Solms (2009) describe information security as *"the discipline used to ensure such protection (of information)"* (Von Solms & Von Solms, 2009) against possible risks to preserve confidentiality, integrity and availability of the information (Von Solms & Von Solms, 2009). Loss of revenue potential, damage to the company's brand, negative publicity, financial fines, and dissatisfied customers are just some of the adverse outcomes of a security breach (Cavusoglu et al., 2015; Ernst & Young, n.d.). Therefore, the ultimate purpose of information security is to preserve the information's CIA through sets of security activities throughout the organisation.

2.3.1 Critical Success Factors of Information Security

An examination of the relevant literature found that a number of distinct elements contribute to the successful deployment of information security. Various factors contribute to the overall efficacy of information security in an organisation that has been explicitly mentioned by researchers, as listed in Table 2.1:

Table 2.1: Critical success factors of information security

	Critical Success Factors of Information Security						
	Top management support	*User training and awareness*	*Security culture*	*Policy relevance*	*Policy enforcement*	*Organisation size*	*Industry type*
Straub (1990)	✓						
Von Solms (2001)	✓						
Dutta & McCrohan (2002)	✓						
Jasperson et al. (2002)	✓						
Kankanhalli et al. (2003)						✓	✓
Knapp (2005)	✓	✓	✓	✓	✓		
Chang & Ho (2006)						✓	✓
Hu et al. (2007)	✓	✓					
Young & Jordan (2008)	✓						

	Critical Success Factors of Information Security						
	Top management support	*User training and awareness*	*Security culture*	*Policy relevance*	*Policy enforcement*	*Organisation size*	*Industry type*
Al-Izki & Weir (2016)	✓						
AlGhamdi et al. (2020)	✓						
Schinagl & Shahim (2020)	✓						

According to the data presented in Table 2.1, the factor with the most significant number of mentions was *Top Management Support*. This indicates that the highest level of management in the organisation is the one that takes charge of leading information system security initiatives and propagates an awareness of the importance of information security among all levels of employees in the organisation. Therefore, top management might have to agree that their commitments significantly impact the success or failure of an information security project initiative (Young & Jordan, 2008).

As mentioned earlier, until the early 80s, information security efforts focused mainly on technical solutions, then moved to the management dimension and slowly shifted to institutional aspects (Von Solms, 2010). Many studies are now exploring the issues of information and cyber security governance (Silic & Back, 2014; Soomro et al., 2016; Von Solms, 2010). It is interesting to see the fact that information security has now incorporated human aspects, which emphasizes the management and governance of information security. This study area has attracted a great deal of interest from experts and scholars and is likely to be investigated for many years.

Since the 2000s, a significant portion of the scientific literature has emphasised the implementation of ISG programs within organisations to furnish protection that is congruent with the objectives and strategies of the organisation (AlGhamdi et al., 2020).

Several studies have highlighted the importance of top management support for enabling information security governance. These studies have focused on the responsibility of top management as well as the primary role that information security governance plays in the organisation's success (AlGhamdi et al., 2020).

2.4 INFORMATION SECURITY GOVERNANCE

Top management now views information security as a strategic issue requiring increased attention, support and motivation. Information security initiatives require direction, goal and aim developed by the organisation's top management, which then escalates and shares by the whole organisation member. When the required activities are implemented to achieve the needs, the top management will receive feedback from all levels of the organisation that becomes part of the monitoring process. This cycle – Direct-Implement-Check- forms a formal structure known as Information Security Governance (ISG), introduced by Von Solms & Von Solms (2009). This cycle is very much aligned with the definition of ISG provided by the international standard on information security governance, which emphasizes the direct and control of information security activities (International Organisation for Standardization, n.d.). This means information security activities require accountabilities and responsibilities at a high level making it imperative to the top management.

There has been a rise in the concept of *information security governance* due to the strategic consideration of information security (Nicho, 2018; Schinagl & Shahim, 2020). Several other terms related to ISG have been defined by previous researchers in addition to the definitions published by the International Standard of ISG. ISG was defined by Posthumus & Von Solms (2004) as a set of procedures that determine how top management handles information security. On the other hand, Moulton & Coles (2003) described ISG as the management of risks connected to information security principles like confidentiality, integrity, and availability by creating and maintaining control environments and the processes and systems that support them. Sajko et al. (2011) identified the term ISG

as a collection of actions demonstrating the amount of engagement shown by the top management and other administrations in an organisation. According to IT Governance Institute (2006), ISG is "a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme".

Therefore, following the discussion on the terminology of ISG, it can be seen that the main objective of ISG is to ensure every level of employees, especially the top management, knows their roles – know what to do, how it should be done and who should do it (Von Solms & Von Solms, 2009; Whitman & Mattord, 2012a; Williams, 2001a). Apart from knowing their roles and responsibilities, top management also needs to understand what security components need to be governed; thus, they can actively engage in information security initiatives in their organisation.

All employees – from top management to junior subordinates, have information security responsibilities (Budzak, 2016; Johnson & Goetz, 2007; Posthumus & Von Solms, 2004; Rothrock & Kaplan, 2018; Von Solms & Von Solms, 2009). Despite the security responsibility of all individuals associated with the organisation, the accountability for managing information security risks and their countermeasures lies on the shoulder of the organisation's top management (Khoo et al., 2010a; Razali & Said, 2015; Williams, 2001a). According to Williams (2001), to fulfil the management responsibility in information security, there are six (6) major activities as follows:

(a) *Policy Development* – The security policy is designed based on the organisation's security objectives and overall mission and vision.
(b) *Roles and Responsibilities* – The duties of the top management and employees are adequately segregated, communicated and understood by all.
(c) *Design* – translate the security policy into procedures, practices, standards and measurements.
(d) *Implementation* – Ensure the employees' implementation of information security initiatives is well executed and maintained.

(e) *Monitoring* – Monitor and control security implementation and compliance measurement and ensure correction and solution for security issues.
(f) *Awareness, Training and Education* – Provide security awareness, training and education to all.

These security activities significantly impacted producing high-quality information security management (ISM) (Soomro et al., 2016). Therefore, top management must be forced to accept the ultimate responsibility to ensure that information security is aligned with the overall business objectives and mission (Budzak, 2016; Von Solms, 2001; Williams, 2001a).

ISG need to be integral but transparent in enterprise governance (also known as corporate governance) (Abu-Musa, 2010; IT Governance Institute, 2006; Von Solms & Von Solms, 2009; Warkentin & Johnston, 2008). This means corporate governance driven by top management is responsible for governing overall business functions, including IT risks (Gale et al., 2022; Kim & Kim, 2015; Slapničar et al., 2023). IT governance (ITG) as one of the corporate governance components appears as a result of expanding the traditional business into ICT for daily business operations Von Solms & Von Solms, 2009; Williams, 2001a). ITG ensures that IT-related risks are appropriately managed and that the reliance on ICT in daily business operations are maintained at all times. ISG becomes a focused activity around information protection to produce a secure environment. On the other hand, ISM has become part of ISG, which involves the management of the operational environment on a daily basis to ensure security policies and procedures are in place Von Solms & Von Solms, 2009). The relationship between corporate governance, ITG, ISG, and ISM can be referred to in Figure 2.3.

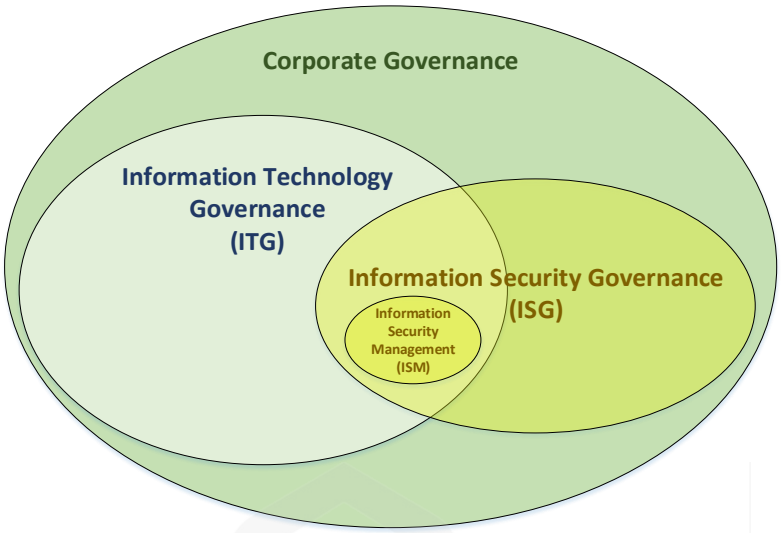


Figure 2.3: The position of information security governance (adopted from Von Solms & Von Solms (2009))

A finding of research conducted by Johnston & Hale (2009) supports the incorporation of information security planning into enterprise governance procedures, which aligns security with other vital business assets and processes that are essential to the success of an organisation. The study also argues that management and employees outside of IT may find it difficult to support or contribute to information security initiatives or to give value to an information security program if security is only perceived as nothing more than an operational component of IT. A more comprehensive perspective and active engagement in information security programs are necessary elements of information security governance (Johnston & Hale, 2009). From this study, it can be seen that information security is more likely to be owned by members of an organisation when addressed in the enterprise planning process. Employees with a greater sense of ownership are more likely to take security seriously and see it not as a hindrance but as a tool that may help them achieve their goals. A more secure computing environment is fostered by increased employee ownership (Johnston & Hale, 2009).

Every key goal in ISG (strategic alignment, risk management, resource management, performance measurement, value delivery) (IT Governance Institute, 2006)

needs direct commitment from the top management. This is because "information security governance is the responsibility of the board of directors and senior executives" (IT Governance Institute, 2006). Thus, top management needs to understand their responsibility and accountability in ITG and ISG and be aware of its importance (Williams, 2001a). According to IT Governance Institute (2006), an established ISG provides many advantages to organisations as follows:

a) Ensure every member in organisations share the same value towards information security and reduce violations of privacy
b) Improve trust and confidence from customers and stakeholders, which increases the organisation's reputation
c) Reduce information security-related risk
d) Optimization of security resources and reduce operational costs
e) Increase the effectiveness of information security policy and its compliance
f) Improve incident response related to security through effective and efficient risk management
g) Critical decisions are made based on a reliable and trusted source
h) Increase accountability in protecting critical business information

If an organisation is able to implement an ISG program, its information security will be enhanced in terms of the quality of top management support, the interaction between business and information security, and information protection (Johnston & Hale, 2009). ISG additionally makes it feasible for responsibility, accountability, and risk controls to be introduced at the level of top management. This helps to ensure that top management will continue to be devoted and supportive of the organisation, and it also makes it simpler to link with the organisation's goals and its protection (Khoo et al., 2010b; Mishra, 2015; Whitman & Mattord, 2012b).

2.4.1 Defining Involvement and Participation

As discussed, top management needs to be actively involved and participate in driving the organisation's information security initiatives and governance. The terms "involvement"

and “participation” are used extensively within the IS field. Although the words are used interchangeably and suggest the same meaning, there is a slight difference between the two, according to researchers in psychology, marketing and organisational behaviour disciplines (Barki & Hartwick, 1989). “Involvement” generally refers to a subjective psychological state reflecting a system’s importance and personal relevance to a user, while “participation” refers to user behaviours and activities. These two definitions are then argued by Jarvenpaa & Ives (1991) in the context of IT, where “executive participation” refers to Chief Executive Officer (CEO) activities and personal interventions in information technology (IT) management. In other words, the CEO spend their time and energy doing the hands-on role of managing IT. Contrariwise, “executive involvement” is more on the psychological state concerning the CEO’s perception and attitudes about IT-related matters, especially his view on IT as a contributing factor to the organisation’s success. Throughout the article, Jarvenpaa & Ives (1991) used “executive support” to refer to the involvement and participation of CEOs.

According to the most prominent online dictionary, the word “engagement” represents “the fact of being involved with something”; or “the process of encouraging people to be interested in the work or an organisation” (Cambridge Dictionary, n.d.). Meanwhile, Oxford Dictionary states the meaning of engagement as “being involved with somebody/something in an attempt to understand them/it; an arrangement to do something at a particular time, especially something official or something connected with your job” (Oxford Learner’s Dictionary, n.d.). Similarly, Merriam-Webster Dictionary defines engagement as “something that engages; the act of engaging; the state of being engaged; emotional involvement or commitment” (Merriam-Webster Dictionary, n.d.). From all the definitions, this study applies the word “engagement” to represent the words “involvement” and “participation” in the IS field. The term top management “engagement” is used widely in this study, and also “involvement”; or “participation” might use interchangeably as this study attempts to explore the influential factors on the engagement of top management in information security initiatives within the Malaysian public sector organisations.

2.4.2 The Role of Top Management in Information Security Governance

Studies by Williams (2001), Von Solms & Von Solms (2009) and Kaur (2016) identified several information security responsibilities which need to be implemented by the top management. Among the prominent roles highlighted by the researchers are setting up directives and formulating policies, providing appropriate security investments and resources, assigning responsibilities to management, providing awareness and training to employees, monitoring information security implementation and measuring improvements in information security programs. It is also the responsibility of the top management to consider employees' perceptions and provide security knowledge for employees to perform their daily jobs and routines in a secure manner (Niekerk & Von Solms, 2010). Table 2.2 lists all the roles and responsibilities of the top management in ISG adapted from Leech (2016), Whitman & Mattord (2012), and Williams (2001).

Table 2.2: The summary of top management roles and responsibilities

No	Roles and Responsibilities
1	Have a sound knowledge of information security
2	Formulate information security policies and directions
3	Ensure alignment between business objectives with IT and risk management
4	Provide appropriate security investments and adequate resources for security programs
5	Define and assign responsibilities to the management level
6	Provide visible support and commitment
7	Provide resources for information security education, training, and awareness programs to employees
8	Set priorities and ensure measurable improvements in information security
9	Monitor and measure information security programs and its implementation

No	Roles and Responsibilities
10	Constantly remind employees about the importance of complying with the information security policy and the implication of not doing so
11	Inculcate security culture by leading through example
12	Subscribe to security assurance from security audit

Among all, setting up an information security policy has been emphasized by many researchers like Singh & Gupta (2019), Singh et al. (2013), Safa et al. (2015) and Kaur (2016). Information security policy consists of written documents describing how an organisation will approach information security strategy and how those approaches directly relate to the organisation's strategic goals (Doherty & Fulford, 2006). For ISG to be implemented effortlessly, the first thing to be done is to produce an information security policy which needs to be clearly defined and documented (Singh et al., 2013). The policy and procedures should also be simple, clear and understandable to all employees. This is in line with the ISO 27001:2013 standards under the "Leadership" clause, whereby top management is required to establish an information security policy compatible with the organisation's strategic direction. A properly formulated information policy is believed to significantly shape information security behaviour in organisations (Safa et al., 2015). Kaur (2016) argues the need to enforce a more rigid information security policy to inculcate security culture and awareness among employees due to the weakest link nature of humans within ISM.

On the other hand, Siponen et al. (2014) provide an approach through the involvement and participation of the top management. They must constantly remind all employees about the importance of complying with the security policy. It can be communicated through electronic mail (e-mails), departmental meetings and training sessions. The training sessions, for example, need to include hands-on exercises as one of the approaches to build confidence among employees to comply with the security policy.

2.4.3 The Importance of Top Management Support in Information Security Initiative

When it comes to protecting an organisation's information, the first line of defence is not hardware or software like firewalls and anti-virus programs; instead, it is the support of top management (Dutta & McCrohan, 2002). Top management support refers to senior leadership's level of understanding and involvement in security activities in terms of the security function (Armstrong & Sambamurthy, 1999; Ragu-Nathan et al., 2004). Consequently, the organisation's top management should take the lead in promoting information security initiatives and raising employees' knowledge of the importance of information security at all levels of the organisation. Continued effort is needed to keep top management engaged in security initiatives when they focus highly on it. Therefore, Kim & Kim (2015) suggests the establishment of an information security committee and identifying the committee's roles in solving internal and external problems of information security, including insufficient top management commitment and support for enterprise-wide information security implementation and activities.

Top management's support and dedication are essential in building policies and processes to effectively manage information security (AlGhamdi et al., 2020; Schinagl & Shahim, 2020; Von Solms, 2001). Al-Izki & Weir (2016) mentioned in their study that the management attitude is a crucial driver of information security governance and can increase organisational information security compliance due to the commitment shown by the top management. As a result, a culture of secure computing practices has been ingrained into the core operations that drive the organisation, resulting in an organisation that is more secure than before (Johnston & Hale, 2009).

Three (3) conjectures were reached by Jasperson et al. (2002) after a review of 81 scholarly articles, where top management support influences the behaviour of other parties and stakeholders in IT decision-making. Also, top management support has a greater impact on the success of projects, and top management support has a more significant effect when there is uncertainty about the importance of IT generally or the project in particular.

Young & Jordan (2008) argue that if the security environment in an organisation is relatively stable, engagement of top management and a clear high-level plan are two (2) key aspects in coordinating behavioural changes in the implementation and compliance of information security within an organisation. A clear high-level plan leads to strategies that offer direction and touch on all parts of the organisation, including financial, research and development, marketing, human resources, and information technology resources (Johnston & Hale, 2009). The policies and procedures of the organisation are mirrored in these strategies, which are then performed as part of the enterprise governance process; the actions that ensure an organisation's strategies are implemented and policies are executed (Johnston & Hale, 2009). As a result of the top management's support and involvement, an organisation's security and organisational culture can be developed, and this motivates employees to carry out their duties (AlGhamdi et al., 2020; Al-Izki & Weir, 2016). When organisations are attempting to harness excellent security rules to turn them into effective practices that turn personnel into strengths rather than risks, the cooperation of top management is highly vital (Alshaikh et al., 2022).

Based on the findings of these researchers, it is possible to conclude that support from top management is capable of influencing the behaviour of an organisation and increasing the level of compliance with information security, which in turn affects the success and efficiency of the implementation of information security initiatives within an organisation. This is why this study focuses on top management, as top management plays a crucial role in information security initiatives.

2.5 INFORMATION SECURITY IN THE MALAYSIAN GOVERNMENT

The setup for this research is based on the structure of Malaysian government agencies and will involve the top management of the agencies. Adopting the definition by ISO/IEC 27000, top management/senior management, also known as executive management, is a "person or group of people who directs and controls an organisation at the highest level. The top management has the power to delegate authority and provide resources within the

organisation" (International Organisation for Standardization, n.d.). Based on the definition, the target group for this research is high-ranked officers in public sector organisations who are directly involved in information security committees/groups like CIOs. In order to obtain various points of view on the subject matter being investigated, this study also conducts interviews with members of middle management as well as officers, directly and indirectly, involved in information security inside their organisation.

2.5.1 Central Agencies Responsible for the ICT and Information Security Initiatives in the Malaysian Public Sector

The Malaysian Administrative Modernization and Management Planning Unit (MAMPU) is an agency within the Prime Minister's Department that plays a crucial role in driving, paving the way, and revolutionising the public service delivery system (MAMPU, 2022). As a central agency for the modernization and transformation of the public service delivery system, it is able to perform six (6) essential functions as below:

a) Proponents and leaders of administrative and managerial modernization for the public sector;
b) Planning and leadership in the development of public sector communications and information technology;
c) Organisational management and information and communication technology (ICT) consultant for public services;
d) Facilitator of the modern service delivery system implementation;
e) Researchers in administrative modernization and public service management planning; and
f) Implementation of the public service delivery promotion system.

Previously, MAMPU was an agency in charge of leading information security in the public sector. However, the national cyber security responsibilities were transferred to The National Cyber Security Agency (NACSA) (MAMPU, 2022).

NACSA was officially founded in February 2017 as the national lead agency for cyber security affairs. Its goal is to secure and build Malaysia's resilience against cyber-attacks by coordinating and integrating the nation's top cyber security expertise and resources (NACSA, 2022). NACSA is also committed to developing and implementing national-level cyber security policies and strategies, protecting Critical National Information Infrastructures (CNII), countering cyber threats, spearheading cyber security awareness, acculturation, and capacity-building programmes, formulating a strategic approach to combating cyber-crimes, advising on organisational cyber risk management, and developing and optimising shared resources (NACSA, 2022). Through these two (2) central agencies, numerous information security measures for the Malaysian public sector are introduced. The three (3) significant initiatives presented by the Malaysian government are explained further in Section 2.5.3.

2.5.2 Mapping of Roles between the Designations of Management Level in Malaysian Public Sector Organisations and ISG Framework

This study attempts to map the designation of management level in public sector organisations onto the ISG framework proposed by Posthumus & Von Solms (2004), as seen in Table 2.3. This is done with the goal of gaining a better knowledge of the management group as a whole.

Table 2.3: Mapping of roles between the designations of management level in Malaysian public sector organisations and ISG framework

ISG FRAMEWORK	DESIGNATION IN MALAYSIAN PUBLIC SECTOR ORGANISATIONS	ICT STEERING COMMITTEE (JPICT*)
Board of Directors	• Secretary General *(Ketua Setiausaha-KSU)*; or • Director General *(Ketua Pengarah-KP);* and • All Deputy Secretary General *(Semua Timbalan Ketua Setiausaha-TKSU);* or • All Deputy Director General *(Semua Timbalan Ketua Pengarah-TKP);* and • CIO	Chairperson: • Secretary General; or • Director General; or • CIO
Board Committees	• ICTSO • All Undersecretary *(Semua Setiausaha Bahagian-SUB)*; and/or • All Head of Department / Division / Unit *(Semua Ketua Jabatan / Bahagian / Unit);* and above	• ICTSO • All Undersecretary *(Semua Setiausaha Bahagian-SUB)*; and/or • All Head of Department / Division / Unit *(Semua Ketua Jabatan / Bahagian / Unit);* and • All Head / Managers of ICT Unit
CEO	• Secretary General *(Ketua Setiausaha-KSU)*; or	

ISG FRAMEWORK	DESIGNATION IN MALAYSIAN PUBLIC SECTOR ORGANISATIONS	ICT STEERING COMMITTEE (JPICT*)
	• Director General *(Ketua Pengarah-KP)*	
Chief Information Officer (CIO)	CIO: • Secretary General *(Ketua Setiausaha-KSU)*; or • Director General *(Ketua Pengarah-KP);* or • Deputy Secretary General *(Timbalan Ketua Setiausaha-TKSU);* or • Deputy Director General *(Timbalan Ketua Pengarah-TKP)*	
Chief Information Security Officer (CISO)	Information and Communication Technology Security Officer (ICTSO): • Head of Information Technology Department / Division / Unit *(Ketua Jabatan / Bahagian / Unit Teknologi Maklumat);* or • Head of Information Security Unit; or • Information Security personnel	
Data Owners	• All Undersecretary *(Semua Setiausaha Bahagian-SUB);* and/or	

ISG FRAMEWORK	DESIGNATION IN MALAYSIAN PUBLIC SECTOR ORGANISATIONS	ICT STEERING COMMITTEE (JPICT*)
	• All Head of Department / Division / Unit *(Semua Ketua Jabatan / Bahagian / Unit)*	

**JPICT: The highest committee established in Malaysia public sector organisations to discuss ICT matters, including information security*

According to Table 2.3, the mapping is constructed using the designation that is used in most government bodies in Malaysia. The Secretary General or the Director General is the person who sits in the top position on the Board of Directors; their deputies follow that order. In most cases, the deputy in a government organisation will consist of two (2) or three (3) deputies, each representing a different branch of administration, development, and several other branches per the organisation's primary function. One of these deputy directors is also the CIO of the organisation.

The Board Committees are represented by each department's Undersecretary or Head of Department within an organisation. According to the type of information utilised and held by each section or department, the department's head, a member of the Board Committees, is also a Data Owner. Typically, the ICTSO of a government agency is the head of the IT department. However, there are also ICTSOs among the head or personnel from the information security unit of the IT department.

The ICT Steering Committee (JPICT) is the highest committee that addresses information security issues in depth. The committee is chaired by the Secretary-General or Director General in several agencies. However, in most organisations, the JPICT chairman is also the CIO, and the CIO is also a member of the Board of Directors. The Board Committees are likewise the same in that they are made up of all department heads as well as all unit managers in the IT department.

In general, JPICT is led by CIO. If the CIO presides over JPICT, and if there are any issues, CIO will bring the matter to other top management knowledge in other meeting platforms. However, if a Secretary-General or Director General chaired JPICT, he had the power to discuss further issues related to information security in management meetings or in JPICT as members of the meeting were the same person. However, meetings involving top management do not have a regular agenda to discuss matters related to information security unless they have issues. Following are the standard information security-related roles and responsibilities of the JPICT's chairman according to document review from all case studies in this research:

(a) Assists the Director General in performing the duties and requirements related to ICT security;
(b) Verifies the ICT Strategic Plan of their organisation which contains the plan to use ICT to support the achievement of the organisation's goals;
(c) Leads the development, operation and management of ICT systems and infrastructure that have integrity and are secure;
(d) Coordinates and manages ICT training and security plans, such as the preparation of the organisation's ICT Security Policy (DKICT) and Risk Management and Auditing;
(e) Responsible for matters related to the organisation's ICT security;
(f) To innovate in electronic government applications, infrastructure and ICT security; and
(g) Implement and coordinate innovation in Electronic Government, ICT infrastructure and security.

On the basis of these duties and responsibilities, it can be determined that the duties and responsibilities of the JPICT Chairman in a public sector organisation necessitate adequate knowledge in administering information security within the organisation. The following section discusses the information security initiatives in the Malaysian government.

2.5.3 Information Security Initiatives in the Malaysian public sector

As far as the history of information security initiatives in the Malaysian government is concerned, it all started when the government began using ICT (such as computers, the internet, e-mail, online systems, and websites, amongst other things) to replace manual systems utilizing the Multimedia Super Corridor (MSC) (Official Portal of MSC Malaysia, n.d.). This transformation is one of the initiatives that the government of Malaysia is doing to modernise, enhance the quality of, and increase the effectiveness of its service delivery, particularly to its citizens, stakeholders, and enterprises.

Observing this development, it is notable that the influence of using ICT has earned a lot of positive advantages, particularly in the efficiency and quality of services supplied by government officials. Despite the improved quality of service, the government of Malaysia has concluded that the increased use of ICT (i.e. the Internet, portals/websites, online applications and many more) poses a more significant threat to information security. In the event that this takes place, it will be detrimental to the nation and may affect the reputation of the government. Because of this, in the year 2000, the Malaysian government issued a circular to all government agencies so that they could implement a security policy known as Dasar Keselamatan ICT Kerajaan (Government ICT Security Policy) (Jabatan Perdana Menteri Malaysia, 2000). This security policy aims to ensure that the ICT systems used by the Malaysian government are kept safe and secure. In general, the policy emphasises sound ICT principles, the responsibility of each agency towards information security, awareness of security risks and threats, and steps to improve the level of information security among organisations in the public sector. The following sections will detail the three (3) noteworthy information security initiatives the Malaysian government has proposed.

2.5.3.1 Adoption of ISO 27001 Information Security Management Systems and the commitment issue of top management

In accordance with its security policy, the Malaysian cabinet issued a directive on the adoption of ISO 27001 Information Security Management Systems (ISMS) in public sector organisations on 24 November 2010 (Jabatan Perdana Menteri Malaysia, 2000). To comply with this directive, each ministry must adopt ISMS, and they will be subject to annual audits by certifying bodies. The roles and responsibilities are outlined on paper, but their implementation reveals a different picture. Initial observations regarding the involvement and participation of top management in information security in Malaysian public sector organisations indicate a lack of commitment on their part.

The problem with top management's commitment was mentioned in a survey on information security carried out by Ernst & Young (2016). The following is what the report stated:

> Cyber resilience requires senior executives to actively take part and lead the React phase. Since 2013, 31% - 32% of responders say there is a lack of executives' awareness and support which is challenging the effectiveness of cybersecurity.

The motivation of top management engagement in information security initiatives has been the subject of research in a limited number of published works. Table 2.4 provides an overview of prior studies by other researchers that are relevant to the research under investigation.

Table 2.4: The summary of top management engagement-related literature

No	Author/Year	Scope/Theme	Sample	Methodology Used
1	Jarvenpaa & Ives (1991)	Examining chief executive officers' behaviours in and perceptions of IT activities.	83 firms were selected from four (4) industries-banking, publishing, petroleum, and retailing in the USA.	Quantitative – Survey
2	Liang et al. (2007)	Examine how top management mediates the influence of institutional forces	77 Chinese firms (private, publicly traded, joint venture, state-owned) –	Quantitative – Survey

No	Author/Year	Scope/Theme	Sample	Methodology Used
		on Enterprise Resource Planning (ERP) assimilation	manufacturing, service, etc.	
3	Hu et al. (2007)	Examine how external and internal organisational influences shape organisational actions for improving IS security	A multi-national company in the United States of America (USA)	Qualitative – Case study (Interview) Semi-structured questions
4	Kajava & Anttila (2006)	Examine the commitment of senior executives to information security	Companies in Finland	Quantitative – Survey
5	Barton (2014)	Examine how external influences motivate senior managers to participate in IS security	SME in the south-central USA	Quantitative – Survey (online survey)
6	Gale et al. (2022)	Examine directors' engagement in cybersecurity	43 Australian organisations across diverse industries	Qualitative – (Interview) Semi-structured questions

This study agrees with previous research, where it is clear that one of the issues still up for discussion is the level of commitment shown by management to information security initiatives. The commitment demonstrated by top management influences the decision-making process regarding implementing information security in organisations and becomes the benchmark by which a successful deployment of information security is measured. However, although top management engagement is critical, numerous past studies have discovered concerns with their commitment, as stated in earlier sections. As a result, by identifying the determinants that influence top management's engagement in information security, this study ensures that all factors are considered in order to improve their commitment to information security.

In reference to the prior research illustrated in Table 2.4, quantitative research methods were utilised in four (4) out of six (6) studies. Even though the involvement of top management is critical in the governance of information security, only a limited amount of research on this topic has been conducted in Malaysia. Therefore, the researcher is motivated to perform studies on top management engagement based on public sectors in Malaysia using a qualitative approach.

2.5.3.2 Public Sector's Cyber Security Framework

Utilizing ICT to improve the delivery of Malaysian government services is one of the steps involved in Malaysia's public sector transformation. This indicates that information and data are stored and processed digitally or cyberspace. Since 2000, numerous circulars and directives concerning cyber security have been issued. However, these instructions are issued separately and contain specifics adapting to challenging technological advancements. Therefore, a comprehensive framework for cyber security is required.

The Malaysian Public Sector's Cyber Security Framework (RAKKSSA) is a fundamental guide and security component that the Ministry and Public Sector Agency should consider in order to safeguard information in their cyberspace. RAKKSSA version

1, dated 1 April 2016, was initiated by MAMPU before the publication was submitted to NACSA on 29 January 2019. The document describes the cyber security framework that the ministry and public sector agencies must use to organise their cyberspace defence (MyGOV, 2022). The cyber security framework aims to provide basic guidance and encompass all the security components that ministries and public sector agencies must consider protecting the information in their cyberspace.

In addition, according to MyGOV (2022), auditing agencies can utilise this document to ensure that information security management plans for the ICT system deployment are comprehensive and assess the system's level of security and maturity. The framework also describes the method for managing official confidential information and the necessity of contacting the office of the Chief Government Security Officer (CGSO) for matters pertaining to the creation, classification, operations, savings, premises, and disposal of information. This framework ensures that suitable security principles are adhered to in light of the necessary risk assessment and processing. RAKKSSA was created for the following purposes:

(a) Ensure that only a complete cyber security framework is used. The number of cyber-attacks and incursions is growing, endangering the country's stability and economy;
(b) Ensure asset protection in accordance with its worth and sensitivity; and
(c) Since 2000, replacing circulars and directives on cyber security have been produced separately and contain specifics that make changing technology difficult (MyGOV, 2022).

Every government agency goes through a process that may be broken down into three steps while developing its cyber security strategy. In order to properly plan for cyber security protection, it is necessary to refer to the document's hierarchy. The direction of the general policy may be found through RAKKSSA and the Public Sector Cyber Security Policy, which serves as the highest level (MAMPU et al., 2016). The document's hierarchy as designated by MAMPU is illustrated in Figure 2.4.

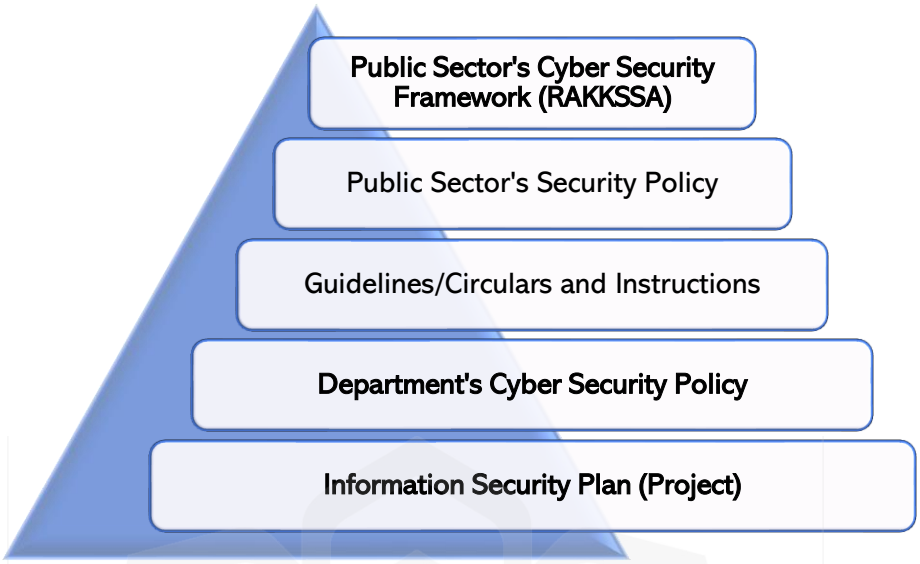


Figure 2.4: The hierarchy of document reference (MAMPU et al., 2016)

Each government agency's cyber security policy is developed in three (3) stages. To plan cyber security protection, the hierarchy of this document must be referred to. According to MAMPU et al. (2016), the order of document references is as follows:

(a) The highest level is the general policy direction provided by RAKKSSA and the Public Sector Cyber Security Policy. Central policies are general and do not change frequently.

(b) The next stage is the Department's Cyber Security Policy, which focuses on the department's specific issues. The department's policies must be reviewed more frequently as technology, demand, requirements, laws, and department functions change.

(c) Lastly, an Information Security Management Plan (Project) is developed to address project operational issues, guided by RAKKSSA, public sector cyber security policy, departmental cyber security policy, and recent circulars or directives. This document includes detailed information on application priorities, access control, and other specific requirements.

RAKKSSA framework provides an overview of all cyber security components that ministries and government agencies should take into account when protecting information in cyberspace.

Subsequently, the ministry and public sector agency of Malaysia will develop their respective departmental cyber security policies based on this framework and the public sector cyber security policy in order to manage and ensure that all departmental activities adhere to the requirements of both documents. To develop information security management plans for ICT projects, all of these documents must be referenced at the project level, and more specific guidelines must be obtained from existing cyber security statutes, regulations, and guidelines.

The framework is based on the existing framework and has been enhanced by the project team of the central agency to produce a cyber security framework for the Malaysian public sector agency. Fundamentally, the RAKKSSA framework comprises eight (8) primary components, as depicted in Figure 2.5.

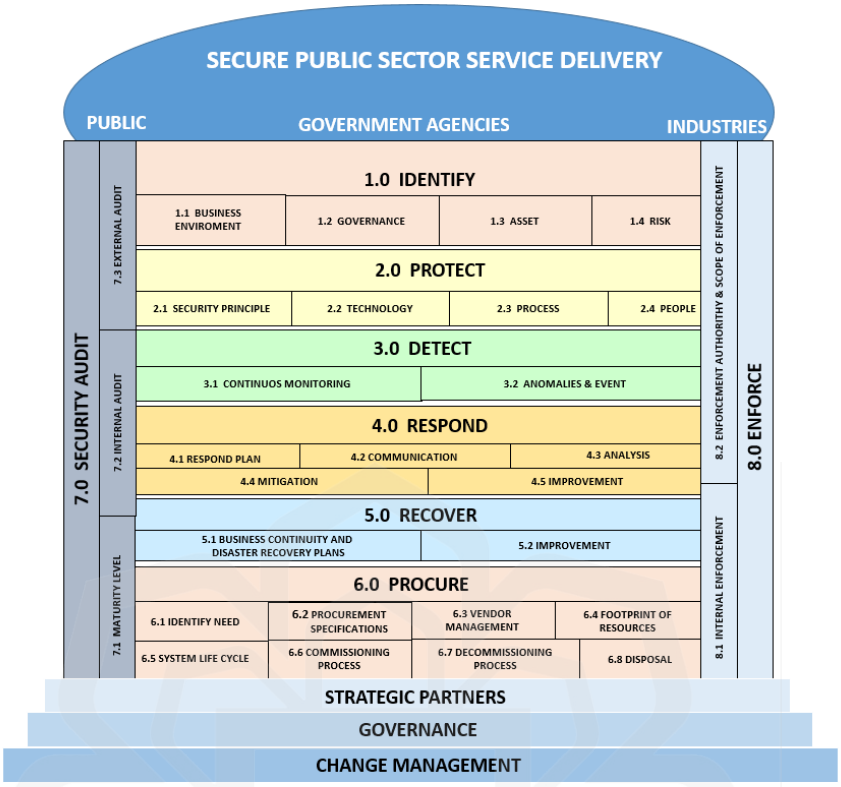


Figure 2.5: Eight (8) main components in RAKKSSA (MAMPU et al., 2016)

The objectives of the eight (8) key components of this cyber security framework are as follows:

(a) **Identify**

It aims to identify the environmental environment, policies and governance structures, and assets that require protection, as well as associated risks and risk management

(b) **Protect**

To develop identified risks, safety principles, technology, processes, and human competencies must be determined

(c) **Detect**

This component's purpose is to detect the threat of malicious code by emphasising the variety of network traffic types and uses

(d) **Respond**

Ensure that action is taken against the threat posed by the malicious code and that the stakeholders and the public are notified (if necessary);

(e) **Recover**

Ensure the availability of information by performing data recovery to the damage caused by malicious code and system failure

(f) **Procure**

Ensure that security controls and requirements are enforced throughout the entire system life cycle for external and internal acquisitions. Important elements include procurement specifications, supplier management, resource traces, system development life cycle, system commissioning, system repair, and system disposal

(g) **Security Audit and** (h) **Enforce**

These two (2) components outline the scope of the audit and enforcement conducted by the Audit Agency and the Enforcement Agency.

Reviewing these eight (8) keys components in the RAKKSSA, one (1) element in the document – Section 2.4 (see Appendix L) relates to "*Manusia* (People)" and contains competency guidelines for the *End-user* and the *Implementer*.

On the other hand, a review of the document reveals that *the RAKKSSA competency components do not include a requirement for the necessary competency for top management.* According to previous research, top management must be in charge of information security governance. Top management is also required to have a particular skill set to fulfil the responsibilities of governing information security initiatives within their respective organisations. It will not be easy to put the governing structure into place if RAKKSSA does not provide a guideline for the competency required for top management. It relates to the issue and problems mentioned in the problem statement of this study (refer to Section 1.3), where information security practices are challenging to implement and appreciate throughout the organisation. This issue leads to three (3) problems where the implementation of information security is often delegated to technical people from the IT unit, top management's engagement in information security initiatives is relatively low,

and information security initiatives are handled as a one-time project instead of a continuous process and improvement.

This study maps the top management's influencing factors on the engagement in information security and the roles and responsibilities of top management in prior literature to a new proposed extension of RAKKSSA focusing on top management competencies. This mapping will be one of the contributions of the research. Further discussion is presented in Chapter Four, Five, and Six.

2.5.3.3 Malaysia's Cyber Security Strategy 2020-2024

The Malaysian government launched the Malaysian Cyber Security Strategy (MCSS) 2020-2024 with an allocation of RM1.8 billion to improve the country's cyber security preparations. The medium-term action plan will be developed, implemented, monitored, and coordinated by the Ministry of Communications and Multimedia (KKMM) and the National Cyber Security Agency (NACSA) (National Security Council, 2020).

According to National Security Council (2020), the strategy was built around five (5) fundamental pillars encompassing 12 strategies, 35 action plans, and 113 programmes as the foundation of cyber security mechanisms for coping with any cyber-attack. The first pillar is to improve the country's cyber governance and security management by upgrading essential ICT infrastructure and increasing the country's ability to address cyber security challenges. The second pillar reinforces existing cyber and legal criminal enforcement by examining relevant laws and adopting specific cyber security legislation. The third pillar is cyber security's empowerment and world-class innovation and technology. In contrast, the fourth pillar focuses on increasing capacity and skilled labour. Finally, the fifth pillar reinforced international cooperation by stepping up regional and international collaboration to safeguard the country's cyberspace.

This proactive cyber defence campaign is essential, particularly in light of the rise in cybercrime during the Covid-19 outbreak. During the period of the movement control order (MCO), the National Cyber Control and Coordination Center (NC4) successfully detected and halted several cyber-attacks on specific agencies, including the Advance Persistent Threat (APT), which is the invasion of particular agency websites, in addition to Ransomware and Zero-day cyber-attacks. With the nation's cyber security plan, uniformity in the adoption and implementation of standards, regulations, and guidelines among all cyber security players in Malaysia can be considerably increased (National Security Council, 2020).

In light of the three (3) measures taken to achieve the objective of information security, controlling national cyber security is an example of a preventive step. Each endeavour features a comprehensive framework, which incorporates governance as well as the involvement of the initiative's executive leadership. Nevertheless, it is necessary to take into consideration the degree to which a variety of parties, most notably the top management, are involved in the administration of this initiative at the ministry and their respective levels. The participation of the top management is essential for the successful implementation of the initiative throughout the organisation. Therefore, this effort aims to encourage researchers to look at the factors that influence top management's engagement in information security activities.

2.6 PLAUSIBLE FACTORS INFLUENCING TOP MANAGEMENT ENGAGEMENT IN INFORMATION SECURITY

Previous sections discussed the significance of top management and critical success factors in implementing information security within an organisation. Despite significant research on information security, studies on governing security are scarce (Nicho, 2018). As mentioned before, research has shown that having support from top management is essential for an information security project to be successful. However, as demonstrated by a study by Veiga et al. (2020), a lack of management support and accountability prompted

this study to explore the plausible factors from previous literature that influenced their engagement in information security governance. Prior to fieldwork, this study's initial research model was constructed using these variables.

According to Chang & Ho (2006), top management's IT competence may affect their attitudes toward implementing security standards and willingness to serve in leadership roles within the ISM. They may also have more confidence in steering proactive security behaviours. This IT competency is intrinsically linked to top management's knowledge via formal education, on-the-job training, or independent study. According to Song (1982), the level of education of top management is one of the characteristics that, in addition to experience and age, influences the level of participation top management has in information security.

In a study that was carried out by Johnston & Hale (2009), the level of influence that various factors had on the participants' decision to implement an ISG program was investigated. According to the findings, concern over civil and legal regulations was the element that had the most significant impact. The other factors are ensuring that the organisation complies with the regulations imposed by the government and protecting the organisation's reputation.

When it comes to influencing the top management's attitude toward information security, Kim & Kim (2015) argue that the information security committee can play a key role and view security as a corporate governance obligation. The study also identifies the roles and functions of each position to help the top management understand their duty in governing information security. Organisation-wide security activities can be achieved once the top management knows their responsibilities and becomes the driver of the implementation.

There are several other variables that, in addition to the criteria that have been described, have the potential to function as determinants that influence the engagement of top management in information security initiatives. These factors are derived in an indirect

manner through the subsequent sections, such as the top management challenges in governing information security, as well as the variables in theory. The theory is utilised as a guide to this study, for instance, the coercive and normative factors mentioned by Cavusoglu et al. (2015) in Part Two of this literature.

2.7 ISSUES IN GOVERNING INFORMATION SECURITY

According to the research by AlGhamdi et al. (2020), support for ISG programs continues to face obstacles. One of these challenges involves the support and responsibility of top management for information security. As for the top management, there are still challenges that they must face in addressing issues involving information security governance.

Firstly, top management always sees information security as an operational and technical issue (Molok et al., 2018; Williams, 2001a). The responsibility to manage the protection of information is often relegated to the ICT department or the small security team in the organisation. This security team is responsible for ensuring security is being executed properly throughout the entire company, which is impossible without support from the top management. When a security incident happens, top management relies on a technical team supporting an existing technological solution to resolve the problem. Top management is reluctant to invest in more effective information security solutions as it would appear to be a waste of funding (Whitman & Mattord, 2012b). The bigger picture behind every incident is often overlooked. Even though the incident might be minor and does not have much impact on the whole business operations, the root cause and corrective actions need to be properly addressed to avoid more severe impacts in the future.

Secondly, top management may not have sufficient ICT knowledge and expertise to give security direction and IT-related strategies (Jarvenpaa & Ives, 1991; Lankton, 2016). Each organisation has security risks, threats and compliance based on the business functions. However, if governance structures and functions are not in place or adequately designed, it is difficult for the employees to exercise due diligence because security

direction is unclear. As a result, it will expose information assets to compromise and reduce their value (Whitman & Mattord, 2012a).

The next issue is that top management does not understand their roles and responsibilities in ISG and ITG (AlGhamdi et al., 2020; Lankton, 2016), which leads to minimal participation in information security initiatives in their organisation (Kim & Kim, 2015). They may be aware of their positions but do not know their accountability, what to do and what to govern. Too few efforts were made to overcome the problem or at least to try to understand it from the strategic level. This result in a much simpler, lazy decision by the top management, leading to the most straightforward solution; subscribing to cyber insurance to mitigate information security issues in their organisation (Horne, 2016).

Lastly, an alternative viewpoint from Kim & Kim (2015) about supporting information security is that it is necessary to make suggestions to top management about things that need to be done for continual improvement. No matter what kind of committee it is, like a steering committee, risk management committee, or compliance committee, the top management should be told about the major security agendas. This part of the information security committee's job will help support information security across the whole organisation. However, it is hard for top management to join the information security committee, even though they are expected to play a key role (Gale et al., 2022; Kim & Kim, 2015; Veiga et al., 2020). IT and security matters are also not included in the agenda of top management meetings (Gale et al., 2022; Lankton, 2016). Even if it is discussed in the meeting, the top management only relies on the reports submitted by the operational executives. However, the reports' contents are generic and high-level, without detailed technical and financial information (Bruin & Von Solms, 2016). Top management also has no time to involve in security as they have many things on their plate (Jarvenpaa & Ives, 1991). Because of this, the top management is not well informed about the organisation's efforts in handling the associated risks (Ernst & Young, 2016). Consequently, decisions made in the meeting may not align with the operational team's current issues. This issue is also related to the lack of direction by the top management due to inadequate security knowledge and strategy (Veiga et al., 2020).

Prior to fieldwork, these discussions provide an early grasp of top management engagement issues in governing information security. It also contributes to the derivation of plausible factors in the initial research model, as shown in Figure 2.11.

In conclusion, the literature review conducted in Part One is crucial to achieving Research Objectives 1, 2, and 3. Part I of the literature review begins with a broad subject covering the definition of information, then the definition of information security, and finally, identifying critical success factors for information security (Section 2.3.1). The scope of the review is then narrowed by concentrating on information security governance (Section 2.4). In this section, the researcher examines the definition of information security governance, which includes the terminology on involvement, participation, and engagement and how these terms are used interchangeably in this study. Finally, the literature review attempts to identify the roles and responsibilities of top management in information security administration, as well as why top management support is crucial in information security. The literature review then attempts to comprehend how information security is implemented in the Malaysian government landscape, as the scope of this study is public sector organisations (Section 2.5). This study also identifies the central agencies in the Malaysian government responsible for bringing information security initiatives to public sector organisations. Understanding information security implementation in the Malaysian government continues, with the researcher attempting to map the ISG Framework from Posthumus & Von Solms (2004) to the organisational structure of Malaysian ministries and agencies. Understanding the preceding can provide a clear picture and background knowledge of the study in order to accomplish Research Objective 1.

Meanwhile, the background research for Research Objective 2 continued by identifying, from previous studies, the factors that influenced the involvement of top management in information security (Section 2.6). These factors are gathered and serve as the foundation for developing the initial research model in Part Two and the basis for developing interview questions for the data collection phase.

The literature review then continues with a discussion of the issues that previous scholars frequently raised to advance understanding of the topic (Section 2.7). It focuses on the challenges that top management and organisations face when implementing security initiatives within their respective organisations. Prior to the implementation of the field investigation, this comprehension is crucial for achieving Research Objective 3.

Elements of the initial research model for this study are derived from the findings of Part One of this chapter, particularly the factors that influence the involvement of top management in information security. The research model's foundation is obtained from concept and theory, which is further described in Part Two.

PART TWO: THEORETICAL BACKGROUND

2.8 LITERATURE MAP OF THEORETICAL BACKGROUND

Figure 2.6 illustrates Part Two of this chapter which presents the theoretical basis for this study, which may help in comprehending the definition and theory needs of the research. As a result, two (2) suitable theories have been employed to investigate the engagement of top management in public sector organisations in Malaysia. Following that, prior literature and theories' outcomes were utilised to construct a research model for this study.

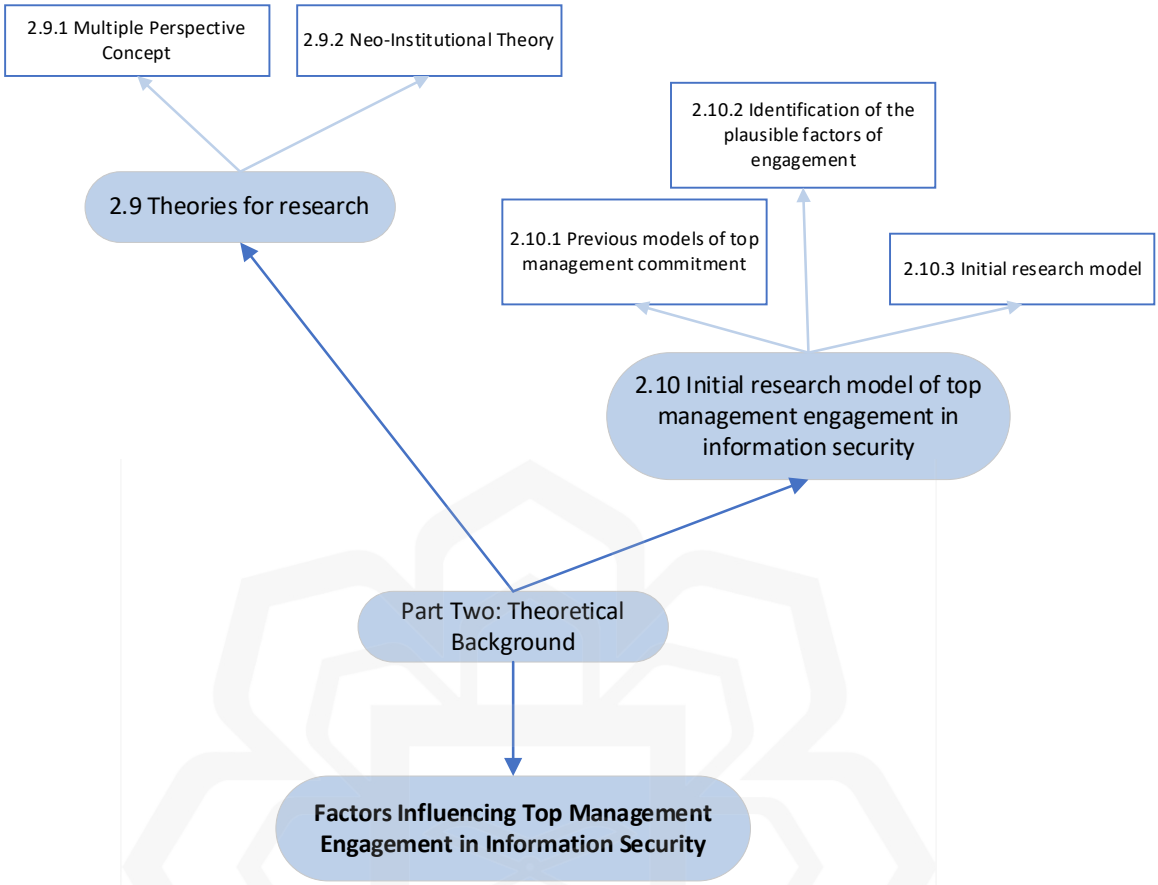


Figure 2.6: Literature map of theoretical background

2.9 THEORIES FOR RESEARCH

For the purpose of describing natural events, a theory is a collection of interconnected variables, definitions, and propositions that provides a unified picture of the world by elaborating on the relationships between its constituent parts (Kerlinger, 1973). Babbie (2016) states that a theory is a well-organized explanation of life's observations. Since the research is required to either test the theories or since the theories are formed by analysing the research data, theories significantly impact scientific inquiry. On the other hand, Bacharach (1989) defines theory as a set of assumptions and restrictions in which a declaration of relations between concepts is made. In a broad sense, each of these three (3) definitions conveys the same information regarding theory. Therefore, the researcher's stance in defining theory is based on these three (3) definitions, where theory consists of a

collection of variables that are related to one another and are described in a structured way that forms a concept that can be understood and explained in related situations.

Theories are used to describe the characteristics and actions of events in the scientific community (Gupta & Sharman, 2009). Researchers develop models that are meant to be representations of reality based on their theories (Pidd, 2003). In order to evaluate the correctness of a theory and provide proof for it, researchers develop hypotheses utilising these models (Gupta & Sharman, 2009). In research, theories are oftentimes employed as a framework for field investigation. Some people use real-world examples to support their theoretical arguments (Gupta & Sharman, 2009). Not many research studies use theories as a framework in their studies, and this is true even in the domain of information system security (Gupta & Sharman, 2009). As a result, a great number of well-established concepts or theories from other fields, including business, management, psychology, and others, are applied.

In research, theory shapes research questions and guides a researcher's focus and understanding (Kaplan & Maxwell, 2005). According to Gregor (2006), there are four (4) goals in applying theory in research – to analyse and describe, explain, predict, or prescribe which lead to the five (5) types of theory as follows:

a) Type I: Theory for analysing
   - A descriptive theory is required when only a few rudimentary facts are known about a phenomenon. Rather than attempting to explain why something happened or forecast the future, an analytic theory simply takes into account existing conditions. Such theories form the groundwork for all others. They summarise the commonalities between several observations in order to characterise or classify various qualities or traits of individuals, groups, situations, or events; as to "what is" at this time.

b) Type II: Theory for explaining
   - These theories focus primarily on the "why" and "how" of certain phenomena. Predicting the future with any degree of certainty is not the primary concern of these theories, however, because of the way they are formulated. This form of

theory can emerge when the how, when, where, and why of past events are explained. This category of theories could be called "theory for understanding" because its primary goal is to help people see the world from a different perspective.

c) Type III: Theory for prediction
   - The "black box" in these predictive theories only explains what will happen, not why. These hypotheses make predictions based on a collection of explanatory factors but don't specify the relationships between the dependent and explanatory variables.

d) Type IV: Theory for explaining and predicting
   - Common conceptions of theory in the scientific and social sciences are consistent with this form of theory, which describes the "what," "how," "why," "when," and "what" of a phenomenon. Without resorting to nomenclature like "scientific-type" theory, which is inappropriate due to the competing ideas within the philosophy of science, it is difficult to identify a suitable short label for this theory class. The name "EP theory" will be used to describe the subject matter covered in this class. In order to describe the theoretical components and the interactions between them, EP theory necessitates comprehension of the underlying causes and the ability to make predictions.

e) Type V: Theory for design and action
   - This type of theory describes how to perform an action. It focuses on the concepts of form and function, methodologies, and justificatory theoretical knowledge utilised in the creation of IS.

In accordance with Gregor (2006), this study makes use of *theory for explaining*. Theories, in this study, are utilised as a basis of the framework and in the process of understanding, specifically, to explain how and why certain events occur. In addition, Gregor (2006) contends that the majority of case study research can be classified under this theory category. Since this study examined four (4) case studies, Type II is deemed suitable to apply. In the next section, the provided theories are employed to explain top management's engagement in information security initiatives.

Information systems, psychology, marketing and organisational behaviour are among the significant fields that provide an in-depth understanding of the concept and definition of involvement and participation in managerial roles in organisations. The development of the initial research model for this study and to address the research questions, this study started with identifying several theories related to managerial and behaviour in organisations. Several of these theories include Multiple Perspectives Concept, Neo-Institutional Theory, and Theory of Administrative Behaviour. The explanation for each potential theory is as follows:

2.9.1 Multiple Perspective Concept

The Multiple Concept (MPC) is a problem-solving approach theory that highlights distinct perspectives on technology-related transformation (Linstone, 1989). These perspectives are referred to as the Technical (T), Organisational or Societal (O), and Personal or Individual (P) perspectives, respectively. These perspectives represent a system via distinct lenses, with diverse sets of underlying assumptions and ideals inherent in each perspective, each offering insights that others do not. The MPC had gained interest from researchers in computer science fields, where several studies utilised this theory. For example, Vidgen (1996) used MP theory to study information systems quality, Yusof et al. (1998) utilised this theory in the information systems implementation plan, and Yusuf et al. (2004) applied this theory in enterprise information systems project implementation.

It is impossible to understand complicated events from a single vantage point completely. The widespread adoption of the Internet, the World Wide Web, and other forms of technology has shifted toward a more global, complicated, and interconnected business landscape, making for a more complex environment in which to operate. This shift has led to a shift toward a business landscape that is more difficult to operate. In addition to internal settings, organisations will also interact with exterior settings, which might significantly differ in culture, politics, society, and economics. According to Mitroff & Linstone (1993), top management needs to embrace a much bigger and more radical style of thinking that

considers a wide range of cultural, technical, organisational, and individual aspects. This way of thinking is required for the management to succeed.

Managers frequently find themselves unable to escape from sets of decisions, each representing a unique set of assumptions about the nature of the problem. Given the complexity of the environment, it stands to reason that incorrect assumptions could result in poor choices. If managers could grasp the varying points of view, they could better direct their efforts toward addressing the concerns of those with the most significant impact on the organisation's success. Therefore, this Multiple Perspective Concept is suited for comprehending the engagement issue of top management governing information security in public sector organisations and needs to take into account the various points of view of employees. Table 2.5 presents more detailed characteristics of the Multiple Perspective Concept based on the T, O, and P lenses adopted from Linstone (1989). The researcher also illustrates all three (3) perspectives of MPC in Figure 2.7.

Table 2.5: Characteristics of the TOP perspectives

	Technical (T)	**Organisational (O)**	**Personal (P)**
Goal	Problem-solving, product	Action, stability, process	Power, influence prestige
Mode of Inquiry	Modelling, data, analysis	Consensual and adversary	Intuition, learning, experience
Ethical basis	Rationality	Justice, fairness	Morality
Planning horizon	Far	Intermediate	Short, with important exceptions
Other characteristics	Cause and effect Problem simplified, idealized Need for validation,	Agenda (problem of the moment) Problem delegated and	Challenges and response Hierarchy of individual

	Technical (T)	Organisational (O)	Personal (P)
	replicability Claim of objectivity Optimization (seek for best solution) Quantification Trade-offs Use of averages probabilities Uncertainties noted (on one hand..)	factored Political sensitivity, loyalties Reasonableness Satisficing (first acceptable solution) Incremental change Standard operating procedures Compromise and bargaining Avoid uncertainties	needs Filter out inconsistent images Need for beliefs Cope only with a few alternatives Fear of change Leaders and followers Creativity and vision by the few Need for certainty
Communication	Technical report, briefing	Language differs from insiders, public	Personality important

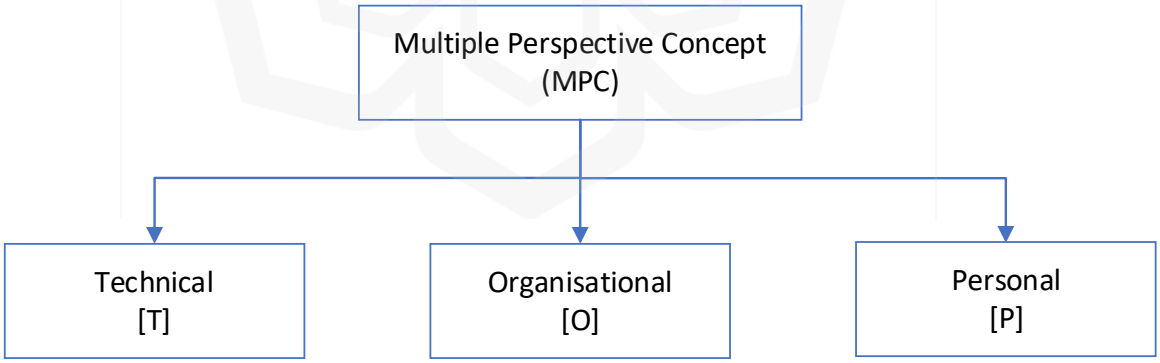


Figure 2.7: The illustration of the TOP lens from the Multiple Perspective Concept

Multiple viewpoints are not without their problems, according to Vidgen (1996). Since the viewpoints cannot be reduced to a common denominator in any meaningful way,

there are no predetermined criteria for weighing the competing needs that emerge from the various points of view. Indeed, the viewpoints may complement, nullify, or highlight competing needs that might serve as a starting point for debate and decision-making. Because of this, a practitioner who employs numerous perspectives must be well-versed in methodologies that accurately reflect the various modes of inquiry and possess the sound judgement to strike a fair balance between them. As for this study, these perspectives are utilised to be the research framework, as depicted in Figure 2.7. Each factor influencing top management engagement is assessed and then grouped under a suitable perspective, which will later be studied through field investigation.

2.9.2 Neo-Institutional Theory

Neo-Institutional Theory (NIT) by DiMaggio & Powell (1983) presented the concept of isomorphism. Isomorphism is developed out of the idea of homogeneity, which describes a process that compels one unit in a population to resemble other units in the population subjected to the same environmental conditions. Isomorphism examines the structural factors that play a role in determining the range of options actors consider logical or sensible.

Institutional isomorphism results in organisations adopting identical structures, strategies, and procedures (DiMaggio & Powell, 1983). This theory explains how institutional forces could shape the behaviour of the organisation's actors (managers) and then determine the organisation's behaviour (Hu et al., 2007a). DiMaggio & Powell (1983) identified *Coercive*, *Mimetic*, and *Normative* as the three (3) primary categories for institutional isomorphism, and they correspond to three (3) separate institutionalisation processes as illustrated in Figure 2.8.

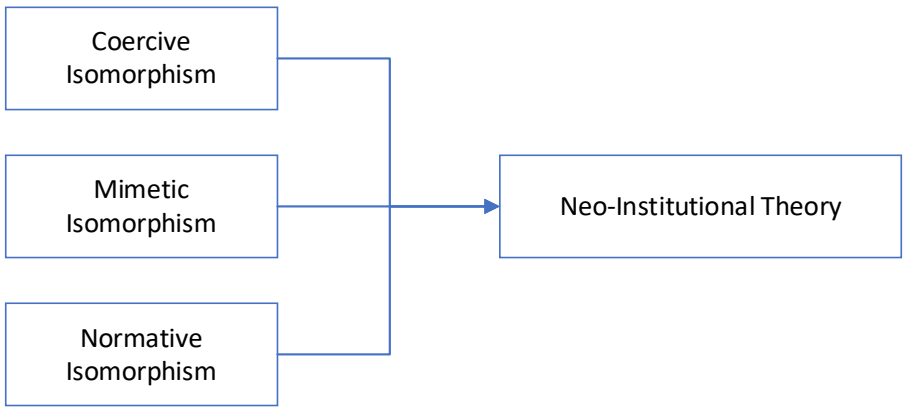


Figure 2.8: The illustration of the three (3) forces of Neo-Institutional Theory

The first isomorphism is coercive. It occurs when organisations accede to the formal and external influences exerted upon them by other organisations, including those on whom they are dependent, as well as the cultural expectations of the society in which the organisations operate; all play a role in shaping the organisations (DiMaggio & Powell, 1983). That means the actor's behaviour is driven by external regulation pressure, for example, government directives, regulations, policies, laws, acts, standards, and the industry and networking outside the organisation.

Meanwhile, mimetic isomorphism is how organisations respond to uncertainty by replicating other organisations' activities. When technologies are unclear, aims are imprecise, or the environment is unpredictable, organisations may model themselves after legitimate or successful organisations (DiMaggio & Powell, 1983). In other words, actors are jumping on the bandwagon to adhere to the achievement of peer organisations or competitors.

Lastly, normative isomorphism is a by-product of professionalisation. It is the effort of members of an occupation to define the conditions and methods of their labour, control the production of future members, and legitimise their occupational autonomy (DiMaggio & Powell, 1983). It is said that formal education and professional networks create a pool of people who can work in any industry. By doing similar jobs in different organisations,

these people have similar attitudes and personalities that make up for differences in traditions and ways of keeping things under control. The actors are forced due to the key persons in the managerial or the actor himself learning (from academic background or professional training) that something is a good thing or needs to do (Bjorck, 2004).

Numerous researches have demonstrated that NIT is capable of providing important insight into the variables that drive organisational transformation or stagnation in an organisation. The NIT has been utilised in various IS and IT research, including those conducted by Cavusoglu et al. (2015) and Hu et al. (2007), about studies on information systems security and the level of information security control resources, respectively. Meanwhile, Hwang & Choi (2017) and Sa & Saner (2011) used this theory to study e-government and e-government information systems security. Jeyaraj & Zadeh (2020) theorizes the three (3) pressures in NIT that influence cybersecurity responses. Gale et al. (2022) analysed primary factors and significant obstacles that influence directors' involvement in cybersecurity.

2.9.3 Theory of Administrative Behaviour

The Theory of Administrative Behaviour refers to the overarching concept that explains how individuals operate within organisational settings (Simon, 1976). According to Simon (1976), individuals in senior positions tend to base their decisions with a greater emphasis on subjective value, whereas individuals in lower positions tend to base their decisions more on objective facts. The top-level of the hierarchy is responsible for making strategic decisions, while the lower level is responsible for making operational decisions. In other words, the top-level is responsible for making "what" decisions, while the lower level is responsible for making "how" decisions. The theory revolves around two (2) fundamental concepts: Bounded Rationality and Satisficing.

The first concept is that of bounded rationality. Bounded rationality acknowledges the cognitive constraints that decision makers face. Simon (1976) contends that the majority

of individuals exhibit only partial rationality, with the remaining portion of their behaviours being driven by emotions or irrationality. He asserts that agents with limited rationality face constraints in their ability to formulate and solve intricate problems, as well as in their capacity to handle information (such as receiving, storing, retrieving, and transferring it) (Simon, 1976).

The second concept is the practice of satisficing. Satisficing is a behavioural pattern that aims to attain a minimal threshold of a specific variable without pursuing its highest attainable value. The term is mostly applied in administrative behaviour, where producers are shown to view profit not as a goal to be maximised but rather as a constraint, in contrast to orthodox economic perspectives. According to these beliefs, organisations must first reach a minimum amount of profit, but after that, they prioritise achieving other goals.

Upon careful analysis of each theory, this study concludes that The Multiple Perspective Concept (MPC) and Neo-Institutional Theory (NIT) are the most suitable theories to be adapted. This study employed the MPC and NIT to explore the influencing factors of top management engagement in the Malaysian public sector. The development of the initial research model for this study can be found in the subsequent section.

2.10 INITIAL RESEARCH MODEL OF TOP MANAGEMENT ENGAGEMENT IN INFORMATION SECURITY

Before beginning work on the model of this study, various models from earlier research were selected from Table 2.4 and referenced. This was done in preparation for the construction of this study's model.

In a study on information system security commitment among top management, Tejay & Barton (2013) utilised Neo-Institutional Theory to analyse the coercive, mimetic, and normative methods through which external factors compel senior managers to participate in ISS. Figure 2.9 depicts the conceptual framework. Mechanisms that are

coercive, mimetic, and normative are distinct conceptions. External impacts and ISS assimilation are mediated by senior management's belief in and participation in Information system security (ISS). The belief of senior management in ISS affects senior management engagement in ISS. Mimetic mechanisms influence the beliefs of senior management and directly affect their engagement. Normative mechanisms directly influence the belief of top management. Their activities demonstrate the participation of senior management in ISS to establish authority and responsibilities, express a vision, and manage, lead and align ISS with the organisational plan. ISS assimilation is the dependent construct.

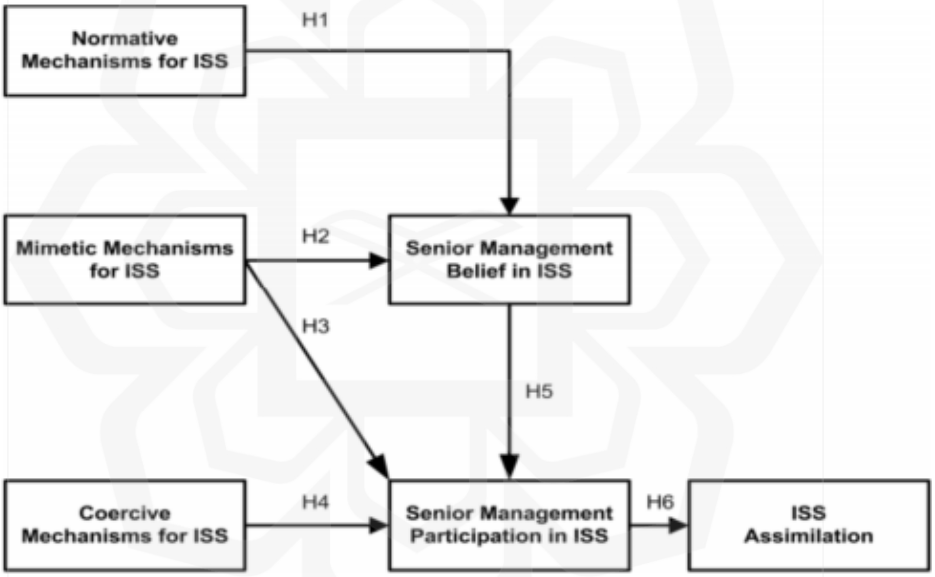


Figure 2.9: A model by Tejay & Barton (2013) on information system security commitment among senior management

This pilot study aimed to determine how external factors encourage senior management to commit to ISS. This study found that senior management could link external influences and ISS integration in organisations. Normative and imitative mechanisms helped senior management's beliefs about ISS. The fact that senior

management believed in ISS made them more likely to take part in it. The involvement of senior management aided the assimilation of ISS.

Another study on enterprise resource planning (ERP) systems by Liang et al. (2007) utilised two things that make up the foundation of their theoretical framework; Institutional Theory and the influence of top management, as shown in Figure 2.10. The theoretical framework is based on the idea that institutional forces affect the way an organisation acts after going through the top management. In the last 20 years, according to them, Institutional Theory has become a powerful way to explain how outside institutions affect how organisations make decisions and what they do. The study argues that institutional forces continue to have an effect on complex enterprise systems as they are put into use and continue to change over time. However, no matter how strong they are, external forces cannot change how an organisation acts unless they first change how the people inside the organisation act. Therefore, the study also mentioned that external institutional forces affect how ERP systems are used through the actions of key organisational members (top management).

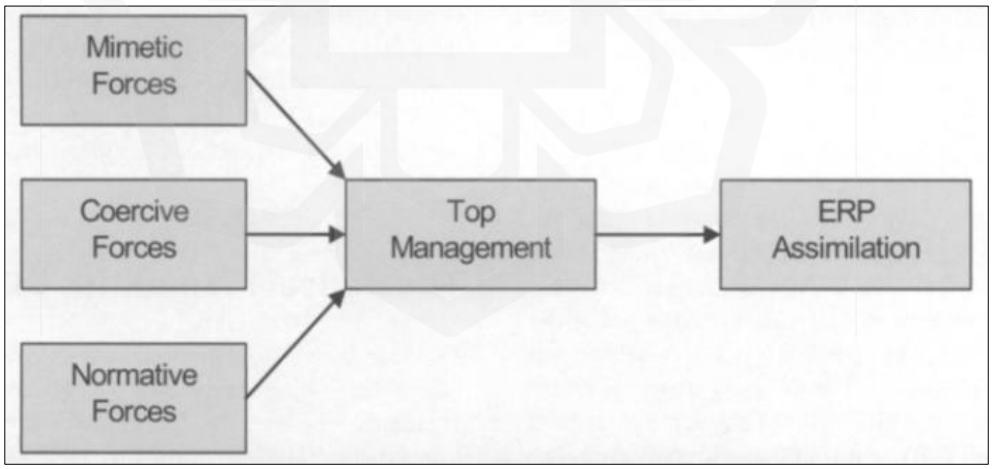


Figure 2.10: A model by Liang et al. (2007) on a study of enterprise resource planning (ERP) systems

Institutional pressures, which are important for adopting and implementing IT, are also significant in the assimilation stage, according to the study. It shows how important it is for top management to help ERP integration by giving in to institutional pressures. Institutional pressures are said to lead to mindless IT adoption, but this research suggests that mindlessness could be helpful for companies that have already implemented ERP systems and want to ensure that all of the ERP system's features are integrated into their business processes.

2.10.1 Identification of the Plausible Factors of Engagement

The foundation of this study's initial research model comprises three (3) elements; the Multiple Perspective Concept as the framework and the forces from the Neo-Institutional Theory. In addition, other plausible factors influencing top management engagement in information security are derived from past literature in Part One: Research Background, as briefly described in Table 2.6.

Table 2.6: The brief description of each factor

No	Factor(s)	Description
1	Regulatory Forces *(Coercive)*	External regulation pressure. For example, government directives, laws, acts, standards, etc.
2	Imitating Good Practice *(Mimetic)*	The tendency to achieve or copy similar accomplishments from peer organisations or competitors.
3	Organisation's Conditions	The organisation's core business, chances for career development, appreciation, and job satisfaction from making important job decisions, significant

No	Factor(s)	Description
		contribution to the organisation's success, freedom in doing work, etc.
4	Organisation's Size	Size often determines the interaction layer between management and employees, the decision-making process and the segregation of duties based on functions. For example, smaller to medium-scale organisations (200 employees or less (Source: SME Corporation Malaysia (2022)) often have direct interaction with the top management.
5	Work Patterns and Practices	The adoption of IT to produce work efficiency, mobility to do work, quality of information security reporting and the platform used to raise information security issues in an organisation.
6	Age	Flexibility to change and adapt to new ideas, new behaviours (young), and delegate of work (old)
7	Formal Education *(Normative)*	Education background from academic institutions or professional course might produce different interpretations and view towards information security.
8	On-the-job *(Normative)*	The job experience or work assignment of top management in the organisation serving in past organisations shapes their role in information security at the current ministry or agency.
9	Informal Education	View, perception, understanding and awareness of the organisation's information security issues might be influenced by self-study, interaction with peer professionals in other organisations, ICT literacy and competency, and security exposure.
10	Tenure in Company	Years of employment and experience in an organisation primarily related to information security.

No	Factor(s)	Description
11	Reputation	To protect and maintain the organisation's reputation and image.

Once all elements are discovered, each one is evaluated and then categorised into the three (3) viewpoints of MPC. Table 2.7 provides a summary of the categorization, which is then utilised to develop the initial research model in the following section.

Table 2.7: The summary of factors categorization mapped into the Multiple Perspective Concept framework

	TECHNICAL/EXTERNAL FACTOR		**ORGANISATIONAL FACTOR**			**PERSONAL FACTOR**			
PAST STUDIES	1) Regulatory Forces *(Coercive)* 2) Imitating Good Practice *(Mimetic)*		1) Organisation's Conditions 2) Organisation's Size 3) Work Patterns and Practices Reputation			1) Age 2) Formal Education *(Normative)* 3) On-the-job Exposure 4) Informal Education *(Normative)* 5) Tenure in Company			
Barki & Hartwick (1989)			Organisation's Conditions						
Jarvenpaa & Ives (1991)			Organisation's Conditions	Organisation's Size	Work Patterns and Practices	Age		On-the-job Exposure	Tenure in Company
DiMaggio & Powell (2000); Meyer & Rowan (1977)	Regulatory Forces *(Coercive)*	Imitating Good Practice *(Mimetic)*					Formal Education *(Normative)*	Informal Education *(Normative)*	
Hu et al. (2007)	Regulatory Forces *(Coercive)*				Work Patterns and Practices			Informal Education *(Normative)*	
Liang et al. (2007)	Regulatory Forces *(Coercive)*	Imitating Good Practice *(Mimetic)*							
Barton (2014)		Imitating Good Practice *(Mimetic)*							
Von Solms (2001)						Informal Education (Perception) *(Normative)*			
Williams (2001)						Informal Education (Perception) *(Normative)*			

	TECHNICAL/EXTERNAL FACTOR		ORGANISATIONAL FACTOR			PERSONAL FACTOR			
Abdul Molok et al. (2013)						Informal Education (Perception) *(Normative)*			
Lankton (2016); Ernst & Young (2016);					Work Patterns and Practices			Competency *(Normative)*	
Horne (2016)								Informal Education (Competency) *(Normative)*	
Chang & Ho (2006)						Informal Education (Competency) *(Normative)*			
Song (1982)						Age	Formal Education	On-the-job Exposure	
Johnston & Hale (2009)	Regulatory Forces *(Coercive)*			Reputation					
Kim & Kim (2015); Veiga et al. (2020)					Work Patterns and Practices		Informal Education (Competency) *(Normative)*		
Gale et al. (2022)								On-the-job Exposure	Informal Education (Normative)

In previous literature, several external factors are believed to influence top management's engagement in information security—for example, the Coercive and Mimetic factors mentioned in the Neo-Institutional Theory and the Regulatory Forces in past studies. However, these *external factors* do not fit the Multiple Perspectives Concept, which describes a scenario from three (3) viewpoints, which are the Technical (T), the Organisational (O) and the Personal (P). For this study to incorporate the external determinants into the multiple perspectives framework, it will be essential to introduce a new perspective termed "External (E)". The study also proposes the External (E) view to merge with the Technical (T) perspective. This merging is justified as the initial study observes zero reasonable determinants under the Technical (T) perspective. This modification to the multiple perspective framework will broaden the study's lens and viewpoint in exploring the engagement issues by the top management. The researcher expects that the initial research model will undergo modifications as new factors are discovered during the field investigation, which will be discussed in Chapter Five.

2.10.2 Initial Research Model of the Plausible Factors Influencing Top Management Engagement in Information Security

Figure 2.11 illustrates plausible factors influencing top management engagement in governing information security initiatives.

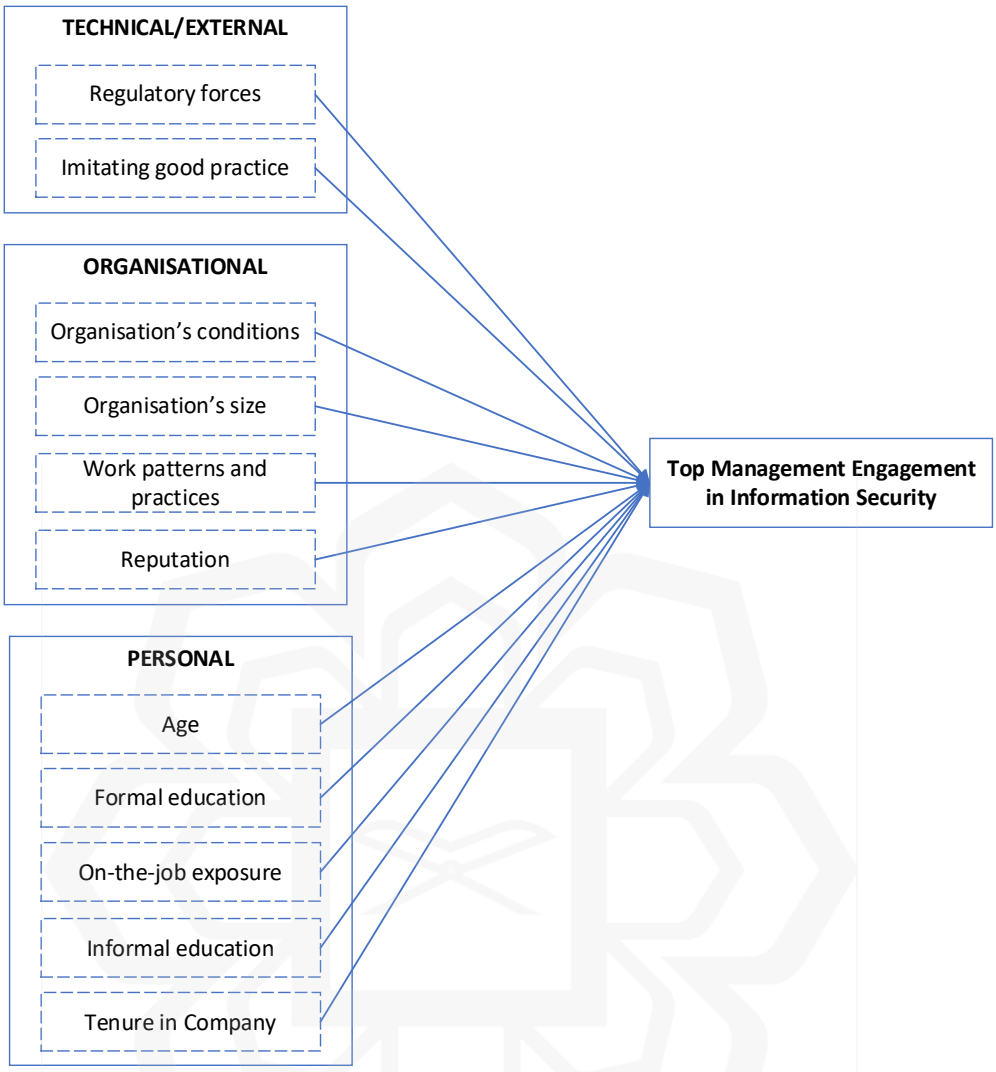


Figure 2.11: The initial research model of the plausible factors influencing top management engagement in information security

Under the "Technical/External" perspective, there are two (2) factors to be studied; Regulatory Forces and Imitating Good Practice. Both factors are extracted from Neo-Institutional Theory which represents *Coercive* and *Mimetic* force, respectively. On the other hand, the factors from the "Organisational" and "Personal" perspectives are extracted from the literature on the involvement and participation of top management in information security. Formal Education, On-the-job Exposure, Informal Education, and Competency under the "Personal" perspective represent the *Normative* force in NIT.

This initial research model highlights several elements from multiple viewpoints that may influence top management participation in information security initiatives. The perspectives aid the researcher in developing the theme for interview questions and then classifying the outcomes, which are addressed in Chapter Four in depth. However, neither the established parameters nor the dependent and independent variables are meant to anticipate engagement concerns. The criteria are intended to offer a fundamental grasp of the investigated issues. The revised model incorporates field investigation study results, and this modification is part of the process of validating the initial research model. It also serves as the final model for this research, as illustrated in Chapter Six.

2.11 CHAPTER SUMMARY

This chapter discusses in detail the past literature on information security, information security governance and the current landscape of information security governance in the Malaysian public sector. To better explain the literature review, this chapter is divided into two (2) parts; Part One covers the research background, and Part Two discusses the development of the initial research model for this study. It started with the literature map, which illustrates the arrangement of the literature review for Part One (Section 2.2). The literature continues with the definition of information, information security, and critical success factors of information security (Section 2.3). This chapter also covers the definition of information security governance, defines the involvement and participation terms, and elaborates on the role of top management in information security governance and its importance (Section 2.4). Next section is the study on information security governance and initiatives within the Malaysian public sector (Section 2.5), and the plausible factors influencing top management engagement are listed based on past studies (Section 2.6). The last topic covered in Part One is issues in information security governance (Section 2.7). Moving on, the introduction of Part Two of this chapter illustrates the literature map of the development of the theoretical framework (Section 2.8). Then, this chapter covers the definition and type of theory and elaborates on the theories utilised for this study (Section

2.9). Last but not least, the final part of this chapter discusses in detail the development of the initial research model, starting from identifying previous models on top management commitment, followed by the identification classification of factors influencing top management engagement according to the Multiple Perspective framework, and finally the presentation of the initial research model for this study (Section 2.10).

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 OVERVIEW

This chapter discusses the selected approach and methods applied in this study, from the research paradigm to the research design. The specific approach and methods are carefully analysed and selected to accomplish the intended objectives and the predicted outcomes. It is arranged as in Figure 3.1.

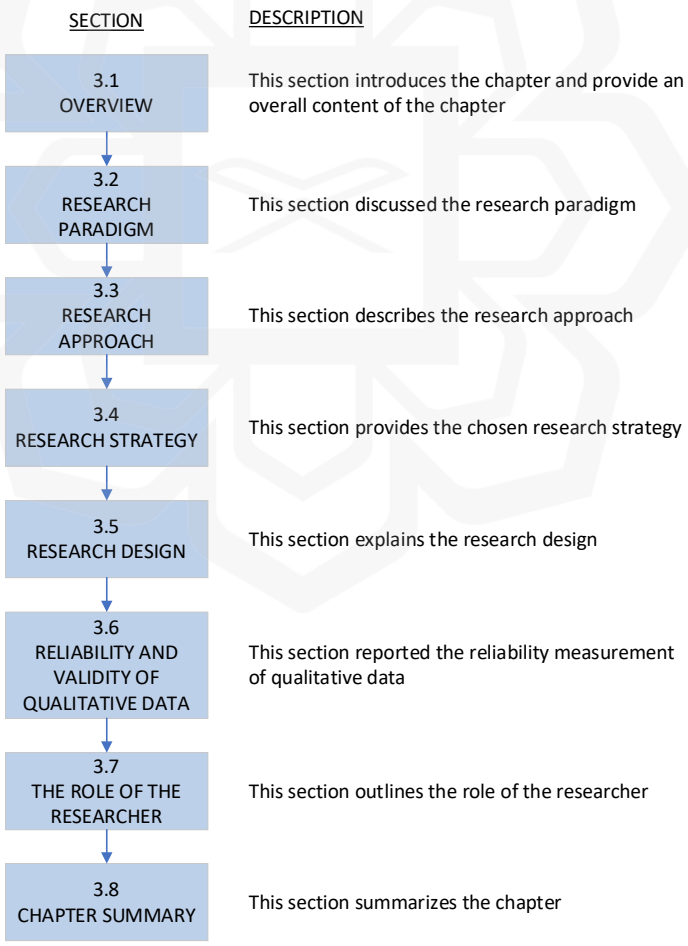


Figure 3.1: Organisation of Chapter Three

3.2 RESEARCH PARADIGM

Every social science researcher adopted a different type of methodological approach. Therefore, it is crucial to identify the appropriate methodology before conducting a study. According to Snape & Spencer (2003), there is no single acceptable methodology for social science research, so it is essential to describe the research philosophy adequately to determine the appropriate methodological approach. Moreover, Benton & Craib (2011) argued that the research philosophy provides the foundations for social researchers in determining appropriate plans, methods, and strategies for any study.

According to Saunders et al. (2016) and Creswell & Creswell (2018), the research philosophy, also known as the research paradigm, is essential for all research areas. It derived from the Greek word *Paradeigma*, which means pattern and was popularized by Kuhn in 1962 in his study to organize the scientific revolution. Kuhn uses the term *paradigm* to demonstrate a conceptual framework shared by the community of researchers, which illustrates a model used to examine problems and solutions. Kuhn also refers to the paradigm as a research culture that consists of beliefs, values, and assumptions, which researchers widely hold as the nature of conducting research (Kuhn, 1970).

Meanwhile, social science has various schools of thought in determining and classifying paradigms. Scholars such as Creswell & Creswell (2018) highlight four (4) paradigms widely discussed in the literature. The paradigms are post-positivism (positivist/postpositivist), constructivism (social constructivism/interpretivism), transformative, and pragmatism. Besides, according to Guba & Lincoln (2005), there are five (5) types of paradigms in qualitative methodological approaches. These paradigms include post-positivism, positivism, critical theory *et al.,* constructivism, and participatory. Table 3.1 summarizes the characteristics of these paradigms, which were adopted from Creswell & Creswell (2018) and Guba & Lincoln (2005).

Table 3.1: The characteristics of Positivism, Interpretivism, Transformative, Critical theory et al., and Pragmatism paradigms

Paradigm	Methodology	Purpose	Method
Positivism also is known as positivist, Postpositivist and Post-positivism	Focus more on quantitative than qualitative approach	To determine outcomes or effects and to test variables	Scientific method
Interpretivism is also known as constructivism social and constructivism	Qualitative approach	To understand the world of social actors through their experiences with the situation being studied	Interaction between participants and researchers
Transformative, also referred to as participatory		Investigations linked to politics and the agenda of political change to deal with social oppression to change participants' lives in which they work or live	
Critical theory *et al.,*		To study the social reality or culture that is historical	
Pragmatism	Mixed-Method approach	Focus on what works and how to solve problems	A blend of scientific methods and interactions between

Paradigm	Methodology	Purpose	Method
			participants and researchers

There are three (3) paradigms that are mainly discussed in information systems (IS) studies, namely Positivist, Interpretive, and Critical Theory *et al.* (Klein & Myers, 1999; Myers, 1997; Orlikowski & Baroudi, 1991). However, only the positivist and interpretive paradigms are discussed in this study. These two (2) paradigms represent the researcher's worldview (Creswell & Creswell, 2018) and guide how they view the world. It is also a belief system about the nature of social reality (Guba & Lincoln, 1994), which is deemed suitable for the study. In addition, Snape & Spencer (2003) argues that to choose a suitable paradigm, researchers shall also consider the ontology and epistemology of each paradigm. Therefore, the following section discusses the ontological and epistemological concerning positivist and interpretive paradigms.

3.2.1 Ontological and Epistemological Consideration

Each paradigm holds elements relevant to a particular research problem, affecting the research process (Creswell & Creswell, 2018; Saunders et al., 2016). According to Guba & Lincoln (2005), the research paradigm encompasses three (3) main dimensions, specifically ontology, epistemology, and methodology. These three (3) dimensions are essential for guiding the entire research process, including selecting methodology and analysis strategies.

Ontology is concerned with the nature of reality (Creswell & Creswell, 2018; Denzin & Lincoln, 2005; Guba & Lincoln, 1994), mainly how the truth and reality are defined (Guba & Lincoln, 1994) and what could be known about it (Saunders et al., 2016). The reality is based on objectivism and subjectivism assumptions (Saunders et al., 2016)

on how researchers view the physical and social worlds (Burrell & Morgan, 2011; Guba & Lincoln, 1994). These assumptions seek to find answers to the nature of social science (Creswell & Creswell, 2018) to constitute the understanding of the world as it is known (Saunders et al., 2016).

On the other hand, epistemology is concerned with the nature of knowledge (Denzin & Lincoln, 2005; Guba & Lincoln, 1994) mainly to understand and explain how truth and reality are known (Creswell & Creswell, 2018; Crotty, 1998; Guba & Lincoln, 1994). Epistemology is based on the assumption that it deals with the best method to study the world (Burrell & Morgan, 2011). This assumption is the relationship between the reality that the researcher is investigating and what the researcher knows (Denzin & Lincoln, 2005). Therefore, identifying, explaining, and justifying epistemological stances is vital for any social science study (Crotty, 1998). Table 3.2 summarises the ontology and epistemology of positivist and interpretive paradigms adapted from Baptiste (2001), Burrell & Morgan (2011), Craig (1998), Creswell & Creswell (2018), Guba & Lincoln (1994), Saunders et al. (2016), Walsham (1995), and Willis (1995).

Table 3.2: The ontology and epistemology of positivist and interpretive paradigms

Paradigm/Dimension	Positivist paradigm	Interpretive paradigm
Ontology	Based on objectivism ontology	Based on subjectivism ontology
	Reality as the objective nature of individual cognition products	The reality of the world understood from subjective experience
	The reality is objective	The reality is subjective
	One true reality	Multiple realities
	Viewed as tangible	Viewed as intangible

Paradigm/Dimension	Positivist paradigm	Interpretive paradigm
	The social science actors and instruments are independent	Gain insight from the social actors' actions and experiences
	Provide robust predictions	No right or wrong theories
	Explanations of reality through observation and measurement	No specific method or single route to knowledge
Epistemology	Based on positivism epistemology	Based on interpretivism epistemology
	Knowledge viewed as an object	Knowledge viewed as a process
	Reality-based on the researchers' external perceptions	Reality-based on the social science actors' thoughts, opinions, experiences, and observations
	The meaning of truth exists independently of conscious mind acknowledgement and experience	The meaning of truth exists through the actors' involvement with realities
	Independent epistemology, where reality is unbiased and independent	The interpretation of meanings is influenced by the researchers' understanding and perceptions
	Testing theory	Developing theory
	Applies scientific language	Adopts interviews in exploring information
	Present facts in statistical terms	Present facts in a normative fashion

Paradigm/Dimension	Positivist paradigm	Interpretive paradigm
	Demands reliability and validity	Demands accuracy and credibility

3.2.1.1 The Ontology and Epistemology of the Positivist Paradigm

The quantitative methodology is associated with objectivism ontology and positivist epistemology (Saunders et al., 2016). According to Burrell & Morgan (2011), the objectivism perspective relates to reality as the objective nature of individual cognition products. It means the reality is given objectively because the knowledge is factual and quantifiable using scientific methods (Saunders et al., 2016) and viewed as tangible in the world of social science (Baptiste, 2001). Besides, the social science actors and the instrument used are independent (Creswell & Creswell, 2018; Saunders et al., 2016), providing robust predictions and explanations of reality through observation and measurement (Creswell & Creswell, 2018).

Likewise, knowledge is viewed as an object of positivism because positivism holds on the standpoint of an objective ontology as it deals with a single reality (Saunders et al., 2016). It is based on the independent epistemology stance because the research dealing with reality is unbiased and independent (Guba & Lincoln, 1994). Since it is based on the researchers' external perceptions (Craig, 1998) thus, the meaning of truth exists independently of conscious mind acknowledgement and experience (Crotty, 1998). Besides, according to Saunders et al. (2016), positivism is involved in designing research built on developing and testing theory-based hypotheses. They argue that positivism applies scientific language and presents facts in statistical terms rather than normative fashion.

Furthermore, positivism demands reliability and validity regarding the real meaning of reality (Crotty, 1998) because its findings are the highest form of knowledge (Saunders et al., 2016) and are recognised as universal (Burrell & Morgan, 2011). Thus, it employs

purely nomothetic methodology as it is the cornerstone of positivist epistemology (Burrell & Morgan, 2011). Crotty (1998) also asserts that positivism can measure and achieve reality by engaging in survey research and employing a statistical analysis methodology governed by strict scientific laws.

3.2.1.2 The Ontology and Epistemology of the Interpretive Paradigm

The qualitative methodology is associated with subjectivism ontology and interpretivism epistemology (Saunders et al., 2016). The subjectivism perspective is the opposite view of the objectivism perspective. For subjectivism, the reality of the world is understood from subjective experience due to it is created by the perception of the social science actors (Saunders et al., 2016). It means the reality is multiple, socially constructed, and from the individual's experience (Saunders et al., 2016), which is viewed as intangible in the world of social science (Baptiste, 2001). Besides, social sciences researchers gain insight from the social sciences actors associated with the situation under investigation (Creswell & Creswell, 2018). It provides a deep understanding of the meaning behind their actions and the world in which they work and live (Creswell & Creswell, 2018). Thus, there are no right or wrong theories because there is no specific method or single route to knowledge (Walsham, 1995; Willis, 1995).

Similarly, interpretivism views knowledge as a process because interpretivism holds a subjective ontology where the social reality is not objective or singular (Bhattacherjee, 2012). It deals with the complex nature of multiple realities shaped by human experiences (Saunders et al., 2016). Since it seeks reality based on the social science actors' thoughts, opinions, experiences, and observations (Craig, 1998) thus, the meaning of truth exists through the actors' involvement with realities (Crotty, 1998). Besides, according to Saunders et al. (2016), interpretivism develops theory rather than testing theory-based hypotheses. Thus, interpretivism adopts interviews to explore information from various actors as different actors have different meanings, although in the same

phenomenon (Bhattacherjee, 2012). For this reason, interpretivism presents facts in a normative fashion (Saunders et al., 2016).

Interpretive epistemology is based on an independent standpoint (Creswell & Creswell, 2018), where meaning is constructed and not discovered (Saunders et al., 2016). The researchers' understanding and perceptions influence the interpretation of meanings because of their direct involvement (Bhattacherjee, 2012). For that reason, researchers must practice an empathetic stance and try to avoid the tendency of bias for their findings to be accurate and credible (Saunders et al., 2016).

3.2.2 The Chosen Research Paradigm

This study aims to explore the influencing factors of top management engagement in information security initiatives among selected Malaysian government agencies. For the study to gather all the determinants, it is crucial first to understand how information security is being implemented in the organisation, up to what extent the top management involve and participate in such efforts, and along the way, what the issues faced by the top management and how the issues may hinder the effectiveness of the information security governance. This study requires comprehensive investigation by engaging the social sciences actors from the government agencies to assemble a detailed and in-depth understanding of the reality. It includes organisation practices, top management actions, personnel experiences, and views on the matter under study.

Some of the previous social science studies related to the engagement of the actors in information systems and security (Barton, 2014; Kajava & Anttila, 2006; Liang et al., 2007a) adopted a positivist approach. The answers are counted and measured in numerical values, thus producing objective output. As opposed to the objective worldview, understanding the complexity of social phenomena requires in-depth conceptualization in which interpretive paradigms fill the gap. The interpretive paradigm is capable of giving

meaningful insights beyond the objective and technical dimension offered by the positivist approach. Therefore, the *interpretive paradigm* is selected to answer research questions and achieve this study's objectives.

3.3 RESEARCH APPROACH

The methodological approach is the plan and procedure that derives from an overall decision on philosophical assumptions, research procedures, detailed data collection procedures, analysis, and interpretation (Creswell & Creswell, 2018). It helps focus on a broad presumption of philosophy to a specific research method for studying a topic. In general, there are three (3) types of methodological approaches commonly used in social science studies, namely the quantitative, qualitative, and mixed-method approaches in which the mixed-method approach blends both elements of quantitative and qualitative approaches (Creswell & Creswell, 2018; Saunders et al., 2016). The following discussion elaborates on the quantitative and qualitative approaches, as both are dominant in today's social science research.

A quantitative methodology is an approach to testing objective theories by studying the relationship between variables usually measured by instruments (Creswell & Creswell, 2018). Since this approach is for testing theories, thus it begins with literature reviews. This approach has an extensive definition in its early stages as those theories and explanations developed from literature reviews (Creswell & Creswell, 2018). Social science researchers use literature review as the foundation for developing research questions, hypotheses, and theoretical frameworks (Saunders et al., 2016) before the relationships or theories are tested and verified using data (Creswell & Creswell, 2018; Saunders et al., 2016).

Besides, the quantitative process is framed using word numbers as it uses closed-ended questions in the form of surveys to collect data, which is later analysed using statistical procedures (Creswell & Creswell, 2018). This approach is against bias as it uses

a deductive style in testing theories (Saunders et al., 2016). Therefore, the findings from this approach can be generalised and replicated (Creswell & Creswell, 2018; Saunders et al., 2016). The quantitative methodological approach has a report writing structure consisting of an introduction, literature review and theory, methods, results, and discussion (Creswell & Creswell, 2018).

In contrast, the qualitative methodological approach develops theories by investigating social life's various phenomena (Denzin & Lincoln, 2005). These theories developed through exploring and understanding the meaning of individuals or groups and complex situations in which social actors live or work (Creswell & Creswell, 2018). Meanwhile, this approach is framed using words as it involves interview sessions and using open-ended questions (Creswell & Creswell, 2018). According to Creswell & Creswell (2018), the categories of information collected during the interview, observation, or another method will be organised into more information units before the data is analysed to form the theme. Inquiries and procedures often emerge while data is accumulated in the participants' settings.

A qualitative process is a bottom-up approach because of the theories developed from information gathered in the field (Saunders et al., 2016). Therefore, this approach adopts an inductive style as it produces themes that arise from interpreted meanings from the data (Creswell & Creswell, 2018). However, this approach has a flexible report writing structure with clearly defined research questions and objectives, but conceptual and theoretical frameworks are not established (Saunders et al., 2016).

3.3.1 The Chosen Research Approach

The research paradigm influences the research practice and guides the selection of the methodological approach (Creswell & Creswell, 2018), and the researcher has chosen the interpretive to be adapted for this study. As for the research approach, Table 3.3

summarizes both methodological approaches to be considered for this study, which were adapted from Creswell & Creswell (2018; Denzin & Lincoln (2011), Djamba & Neuman (2002), and Saunders et al. (2016).

Table 3.3: The comparison between quantitative and qualitative methodological approaches

Quantitative	**Qualitative**
Pre-determined	Emerging methods
To test objective theories	To develop theories from information gathered in the field
Studying the relationship between variables	Exploring and understanding the meaning of individuals or groups;
Framed using word numbers	Framed using words
Closed-ended questions	Open-ended questions
Based on the deductive style	Based on the inductive style
Performance data, observational data, attitude data, census data	Interview data, audio-visual data, observation data, document data
Conduct surveys to collect data	Conduct interviews, audio-visual, observation, and document analysis to collect data
Analysed using statistical procedures	Text and image analysis
Findings can be generalised and replicated	Themes, patterns, and interpretations mostly cannot be generalized and replicated
Has a set report writing structure	Has a flexible report writing structure
Begins with a conceptual or theoretical framework and an extensive definition	Usually, do not begin with conceptual, theoretical frameworks and extensive definition

Given that the study is concerned with top management engagement in information security initiatives within government organisations, all participant information (including information security and non-information security personnel) is collected in their respective environment settings. A more in-depth understanding and a more comprehensive image are provided by the qualitative approach combined with the inductive approach in the study (Merriam, 2009). According to Avison et al. (1999), qualitative research methods effectively explain what occurs in organisations, and as a result, this method can be employed in this study to explain how information security governance is practised in Malaysian public sector organisations. Therefore, *the qualitative* combined with an inductive approach is the most suitable methodological choice for this investigation. The overview of the chosen methodology is shown in the following Table 3.4.

Table 3.4: The selected methodology

Methodology	**The Selected Perspective**
a) Ontology	Subjectivism
b) Epistemology	Interpretivism
c) Research Paradigm	Interpretive
d) Methodology Approach	Qualitative with Inductive Approach

3.4 RESEARCH STRATEGY

The research strategy, alternatively referred to as an inquiry strategy or research design (Denzin & Lincoln, 2011), is a specific sort of inquiry based on a particular methodological technique (Creswell & Creswell, 2018). Due to the qualitative technique chosen for the study, this section examines the nature of the study within this approach. This debate is critical since it outlines precise techniques for conducting social science research (Creswell & Creswell, 2018).

Qualitative research strategies are utilised in various ways in social science research. Nonetheless, there are five (5) most frequently used and popular strategies: narrative research, ethnography, phenomenology, grounded theory, and case study (Creswell & Creswell, 2018; Saunders et al., 2016). Table 3.5 outlines the characteristics of these five (5) research strategies prior to selecting the most appropriate one.

Table 3.5: The characteristics of research strategies

Research Strategy	Objective	Type of study
Narrative research	To study the lives of one or more individuals concerning their life stories.	Researchers connect themes into a storyline by organizing the story of one or more individuals' lives in chronological order using plot, setting, activity, climax, and sequence as fundamental tools to restore participants' life stories.
Ethnographies	To study the board patterns of culture-sharing behaviours, language and actions by entire cultural groups in the natural setting over a long period.	Researchers generate a detailed portrait of a cultural-sharing group through numerous interviews, observations and explorations of a single cultural group artefact. This design often introduces literature on cultural concepts or critical theory in the early stage of a proposal or report as an essential framework.
Phenomenology	To study the life experiences of several individuals about the phenomenon as	Researchers express a general or detailed description of the participants' life experiences by analysing the significant statements, generating meaning units, and developing a story of the essence. This

Research Strategy	Objective	Type of study
	described by the participants.	design often uses minimal literature and usually employs three to ten participants for interviews.
Grounded theory	To discover a general or abstract theory by exploring processes, actions, activities, and events grounded in participants' views and assigning it as their studies' conclusion.	Researchers generate a theory from data by using multiple stages of data collection, starting with directing questions to explore. Then creating categories of information based on systematic steps (open coding), filtering the information by selecting one category and putting it in a theoretical model (axis coding), and lastly, clarifying a story from the link between groups of data (selective coding). This design often uses minimal literature because it does not guide and direct this study. However, literature often helps once patterns or categories have been identified. Usually, this design employs twenty to thirty participants for interviews or until the data are saturated.
Case study	To explore inquiry of one or more individuals' cases, programs, processes, activities or events in various fields, especially evaluation by developing an in-depth case analysis.	Researchers use a variety of data collection procedures to collect detailed information over a sustained period, as cases are bounded by time and activity. It starts with addressing the specific questions of the situation as it involves a detailed description of the setting or individual and then data analysis to identify particular themes or issues. A case study often uses minimal

Research Strategy	Objective	Type of study
		literature and usually employs four to five cases until the data are saturated.

3.4.1 The Chosen Research Strategy

The case study is a research strategy involving a study to explain a phenomenon in its setting where researchers are interested in studying "why" and "how" questions from smaller groups of entities consisting of people, groups, or organisations (Benbasat et al., 1987; Gray, 2004). Case studies use various data-gathering methods to obtain information about one or more individuals, groups of people, an entire program, an activity, or an organisation inside a constrained system (Benbasat et al., 1987; Creswell & Creswell, 2018). It is possible to do case studies on a single or a series of instances with varying analysis degrees (Yin, 2018). These include interviews, focus groups, document analysis, surveys as well as other methods of data collection. Individuals or groups within the research setting are also used to collect data.

Due to the limited number of cases studied, case study results cannot be statistically generalized (Stake, 2006). Refining theory, proposing further investigation, and helping to illustrate the limitations of generalizability are some of the benefits of case studies, according to Stake (2006). Rather than generalizing, qualitative case studies focus on the particulars of an experience (Patton, 2002; Stake, 2006). For these reasons, *the case study research method* suits this research. A case study allows a deeper understanding of the issues and problems under study. Case study research's ability to draw on a wide range of sources of information is one of its greatest strengths (Benbasat et al., 1987; Yin, 2018).

3.4.1.1 The Single and Multiple-Case Study

Several scholars classify case studies into two (2) types of design, namely single and multiple-case studies (Merriam, 2009; Stake, 2006; Yin, 2018). Therefore, before conducting a study, it is essential to determine whether it used one or more cases because both studies have different designs (Yin, 2018).

A single case study resembles a unique experiment that analyses specific contexts without linking them to other cases. It is ideal for studying a critical, extreme or unusual situation, unique and one of a kind (Saunders et al., 2016; Tobi, 2016). Besides, a single case study also provides an opportunity to analyse previously inaccessible phenomena (Saunders et al., 2016) or be used as a pilot case before starting a multiple case study (Yin, 2018). However, if studies do not meet these conditions, researchers are not encouraged to use this design, as it lacks the ability to be replicated and is vulnerable and like putting all the eggs in one basket (Yin, 2018).

Yin (2018) suggests that the case study incorporates more than one case study to replicate the findings. According to Yin (2018), replication is the conclusion of a case, in which results will be compared to determine whether it is similar or different from the outcomes of another case. There are two (2) types of replications; literal replication and theoretical replication. A literal replication suggests that the selected cases are similar for predicting similar results, while a theoretical replication is based on the presumption that the chosen case predicts contradictory results (Yin, 2018). Nevertheless, Yin (2018) asserts that both replications are intended to strengthen the case study's findings by drawing reliable conclusions for the research.

Merriam (2009) and Yin (2018) also emphasized that to make the analysis of a case study more compelling and convincing, researchers need to have more than one case because multiple cases overcome weaknesses in employing a single case as it provides substantial analytical benefits. Therefore, scholars such as Saunders et al. (2016), Stake

(2006), Tobi (2016), and Yin (2018) suggest that researchers use multiple case studies if the research has cases of similar characteristics.

Furthermore, multiple case studies provide a distinct advantage to the investigation as it allows for evidence from numerous sources (Tobi, 2016) before coming to a "cross-case" conclusion (Yin, 2018). Thus, it is considered more robust (Herriott & Firestone, 1983) because the findings' accuracy, validity, and stability can be strengthened (Merriam, 2009). On the other hand, multiple case studies also intensify external validity, showing that the findings can be generalized (Merriam, 2009; Yin, 2018). Consequently, Tobi (2016) asserts that although both designs can help achieve the aim of this study, multiple case studies are preferable.

As this study focuses on four (4) public sector organisations in Malaysia with different business functions, by studying several ministries/agencies, the research outcome produces robust, powerful data and strengthens the findings. As a result, it allows a deeper understanding of the issues and problems under study. Multiple case study research's ability to draw on a wide range of sources of information is one of its greatest strengths (Benbasat et al., 1987; Yin, 2018). As one of the goals of this research is to understand the multiple views of participants inside an organisation, a *multiple-case study* is a good fit for the research.

Furthermore, the multiple-case study adopted by this research is used as *part of validating the initial research model* developed in Chapter Two. Establishing an initial research model provides multiple perspectives for a more in-depth understanding of the factors that influence the participation and involvement of top management in information security initiatives derived from the past literature. Then, the viability of the initial research model is demonstrated by its application in conducting the field investigation of actual case studies. Findings from the case studies provided evidence of the initial research model, particularly the factors influencing top management engagement in information security. The process of validating the model includes alterations and modifications to the initial

research model based on the findings and evidence from the multiple-case studies. As a result, the initial research model becomes a qualitative validated model. In this research, a multiple-case study is employed as part of the procedure for validating the initial model.

3.4.1.2 The Unit of Analysis

As this study adopted a multiple-case study design, the unit of analysis in the case study is referred to as the case, in which the case consists of an individual, small group, organisation, event, entity (Yin, 2018), artefacts, any bounded system determined by the researcher or interactions among individuals (Merriam, 2009; Stake, 2006). Additionally, (Yin, 2018) classifies the unit of analysis for single or multiple case studies as either holistic or embedded.

In a holistic design, the unit of analysis is considered to be one or a subunit. The holistic design only studies a single case within a single or multiple case study design (Yin, 2018). The individual case is considered the whole single case study as it analyses the global nature of a program or an organisation. Meanwhile, in the embedded design, the unit of analysis is considered multiple or subunits. Therefore, the embedded design studies more than one case within an individual or multiple case study design (Yin, 2018), in which the combination of the numerous cases is considered the whole individual case study. The embedded design is used to enhance insights, add great opportunities for comprehensive analysis, and become an essential tool for maintaining the focus of the research (Yin, 2018).

This study requires further evidence coming from various sources of data. It is to ensure sufficient information can be gained to provide a detailed and accurate understanding of the top management engagement in information security, the factors of their engagement, and the issue that revolves around information security governance in multiple ministries or agencies of the Malaysian public sector. Therefore, the use of embedded design enables this study for a broader collection of data in the individual case

study within the multiple case studies design. Furthermore, it allows the researcher to identify subunits of evidence that enrich knowledge, prevent unexpected spillages, and enhance the focus of the research, which eventually leads to a more precise level of inquiry (Yin, 2018). Thus, this study employs an *embedded design* to achieve the aim of this study.

An embedded multiple case study requires the researcher to determine what, who, when, and where the observation or interview will be conducted (Merriam, 2009). Accordingly, some scholars have suggested using a sampling strategy in determining this selection (Creswell & Creswell, 2018; Merriam, 2009; Patton, 2002; Saunders et al., 2016). It is essential to choose the appropriate sampling method based on the subject population, research considerations, research design, and research approach so that the selected sample truly represents the population of interest (Saunders et al., 2016). Furthermore, this ensures that the conclusions drawn from that sample can be generalized back to the selected population (Bhattacherjee, 2012).

3.4.1.3 The Sampling Techniques

Generally, there are two (2) types of sampling methods; probability sampling (or representative sampling) and non-probability sampling (or judgmental sampling) (Saunders et al., 2016). Probability sampling is a random selection that offers the chance for each case in the population to be equally selected (Creswell & Creswell, 2018). Probability sampling is commonly used in quantitative studies involving survey and experimental research strategies (Creswell & Creswell, 2018; Saunders et al., 2016).

On the other hand, non-probability sampling methods provide researchers with various alternative techniques for selecting samples based on the researcher's subjective assessment (Creswell & Creswell, 2018; Saunders et al., 2016). This method is efficient when research questions and objectives require exploratory research by conducting in-depth research or focusing on small cases to enrich information and gain new insights

(Saunders et al., 2016). The non-probability sampling is commonly used in qualitative studies involving quota sampling, convenience sampling, purposive sampling, self-selection sampling, and snowball sampling (Saunders et al., 2016).

This study aims to explore information security governance in the Malaysian public sector. Therefore, this study explores to gain a detailed and accurate understanding of how top management engages in information security initiatives in their organisation, the factors influencing their engagement, and the issues in information security governance. Thus, this study employed *purposive sampling*, as it is the most appropriate technique for studying case studies (Merriam, 2009; Saunders et al., 2016) and because it identifies and chooses individuals who are genuinely knowledgeable and experienced in this study phenomenon (Denzin & Lincoln, 2011; Saunders et al., 2016).

3.5 RESEARCH DESIGN

Research design is defined as "types of inquiry within qualitative, quantitative, and mixed methods approach that provide specific direction for procedures in a research design" (Cresswell, 2014, p.12). Research design provides a structure where all elements and strategies, from the beginning (initial questions) until the end (conclusions to be drawn), are bonded and linked together to guide researchers in conducting their studies (Yin, 2018). As mentioned earlier, the study adapts the multiple-case studies method Yin (2018) proposed, as illustrated in Figure 3.2. The research design, which is intended to answer the research questions, is divided into three (3) phases, as depicted in Table 3.6.

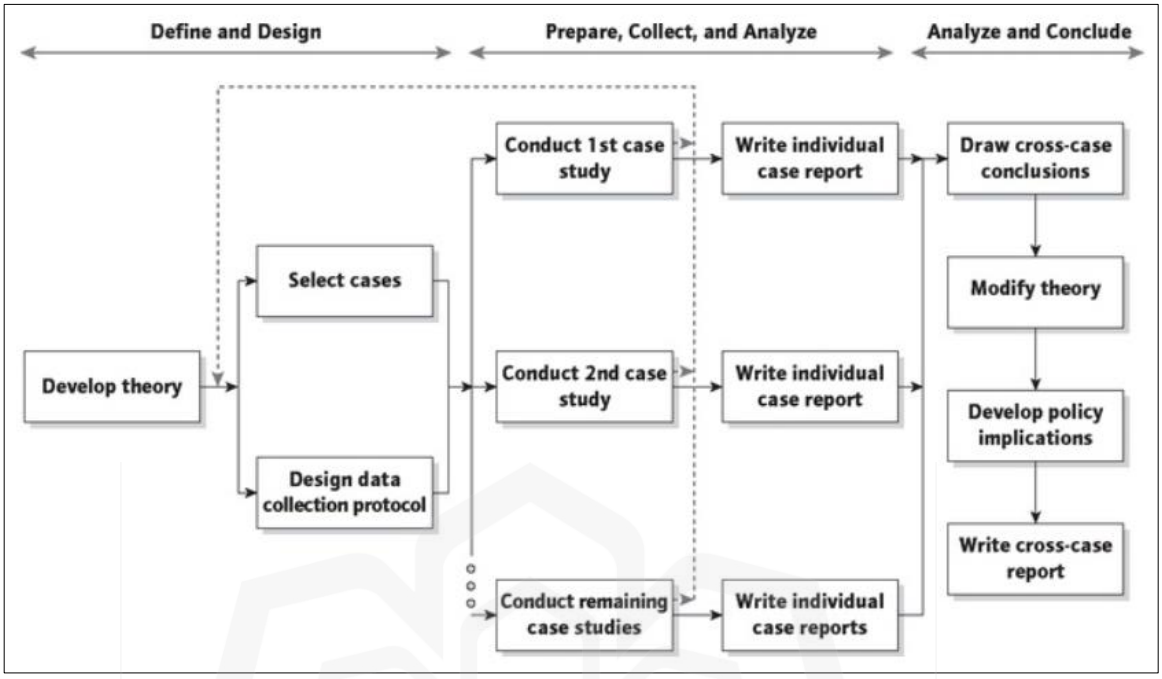


Figure 3.2: Multiple-case studies method

The steps that should be taken along the study path are outlined in the research design, which leads researchers through the process. A sound study design will reduce the likelihood of researchers becoming disoriented during the course of the research. The five (5) significant phases of the study are as follows:

- Phase I: Contextual Study
- Phase II: Preparation for Field Investigation
- Phase III: Field Investigation
- Phase IV: Thematic and Single-Case Analysis
- Phase V: Cross-case Analysis and Conclusion

It may appear that the study is organized into phases because of the research design. However, it is more iterative and adaptable in reality. Some actions in the phases are modified based on the study requirement, phases are revisited as needed, and fresh inputs are brought into the research process iteratively in this study. Especially in an interpretive

multiple-case study where the goal is to gain a comprehensive understanding of a phenomenon, in this case, information security governance of the top management in the Malaysian public sector, these procedures are unavoidable. In order to address the research question, it is necessary to study the literature, improve the instrument, and return to the field to gather additional data.

Table 3.6: The research design

Multiple-case Studies Method by Yin (2018)	Research Phase	Research Process	Method	Activity	Deliverable
Define and Design	Phase I: Contextual Study	Contextual Definition & Concept	• Database/ Web searching for journals and papers • Books reviews	• To identify the research issue & problems, objectives, questions, and scope • To review past literatures, theories, models • To propose an initial model • To identify the research paradigm and the suitable methods to conduct the research • To outline research design	• Problem statement, RO, RQ, research scope *(Chapter 1)* • Literature reviews on information security governance, MPC, NIT, information security in Malaysian government context *(Chapter 2)* • Initial model of the factors influencing top management engagement in

Multiple-case Studies Method by Yin (2018)	Research Phase	Research Process	Method	Activity	Deliverable
					information security *(Chapter 2)* • Identified research methodology • Established research design *(Chapter 3)*
Prepare, Collect, and Analyze	Phase II: Preparation for Field Investigation	Information gathering	• Websites searching • E-mails • Phone calls and text messages	• To identify suitable organisations and potential interviewees (4 organisations) – purposive sampling • To contact organisations, get the approval to carry out the interview	• Case study protocol • Refined interview questions • Instruments for interview o Confirmation letter o Consent form o Interview checklist o Demographic survey form

Multiple-case Studies Method by Yin (2018)	Research Phase	Research Process	Method	Activity	Deliverable
				• To contact "gatekeeper" from all organisations to set up appointment dates for each interviewee (27 participants) • To formulate interview questions (semi-structured) that applicable to all participants within 3 designations • To conduct a series of mock interviews and refine interview questions	○ Contact summary ○ Observation checklist ○ Document review form ○ Voice recorder ○ Other related documentations • Access grant

Multiple-case Studies Method by Yin (2018)	Research Phase	Research Process	Method	Activity	Deliverable
				• To design the other instruments for data collection	
Prepare, Collect, and Analyse	Phase III: Fieldwork **	Multiple-case Studies	• Interview • Document review • Observation	• To conduct interviews at 4 organisations consisting 27 participants • To gather information from document reviews and observations • To arrange data gathered from the interview sessions • To follow-ups with participants	• Completed demographic survey forms • Interview notes including document review and observation notes • Voice recorded interview sessions (between 21 minutes 41 seconds to 1 hour 32 minutes 51 seconds)

Multiple-case Studies Method by Yin (2018)	Research Phase	Research Process	Method	Activity	Deliverable
					• Other related documents obtained from the interview sessions
Analyse and Conclude	Phase IV: Thematic and Single-Case Analysis	Data familiarization and analysis	• Atlas.ti 22 • Microsoft Excel	• To transcribe recorded interviews (verbatim) • To familiarize with the transcriptions • To code and categorise data • To conduct inter-coder reliability • To retrieve single-case findings	• Interview transcripts • Codes, categorisations, data reduction, data display • Inter-coder reliability results • Triangulation within single case • Single-case findings

Multiple-case Studies Method by Yin (2018)	Research Phase	Research Process	Method	Activity	Deliverable
	Phase V: Cross-case Analysis and Conclusion	Analysis and finalize findings	• Atlas.ti 22 • Microsoft Excel	• To identify themes and sub-themes • To identify emerging findings • To retrieve cross-case findings • To modify the initial model based on the findings • To validate findings by triangulate within single case and by designation (cross-case), document reviews and observations • To draw conclusions	• Cross-case findings (similarities, differences) • Ranking for factors (most quoted to less quoted) • Final model of the factors influencing top management engagement in information security • Conclusion

Based on Table 3.6, this study's research design is based on Yin (2018). The details of the research design implementation are presented in the following sub-sections.

3.5.1 Phase I: Contextual Study

People who have direct expertise in the information security industry, including information security auditors, are a significant source of information in identifying the research problem for the first phase of this project. The researcher's previous experience, observation, and initial understanding of the study also contributed to identifying the research problem. Following that, the literature and related theories gained greater insight and clarification. The research scope was defined, the research paradigm was identified, and a research strategy was subsequently outlined to complete the study. Then, the researcher developed a problem statement and a set of study objectives after thoroughly reading and analysing the relevant literature. In addition, models and ideas that might be useful were discovered, and an initial research model was sketched out. While still in its infancy, this phase represents an important step toward achieving the research objectives, especially in identifying plausible factors of top management engagement in information security.

3.5.2 Phase II: Preparation for Field Investigation

Phase II is the initial data collection phase in the study prior to the field case studies. This phase's objective is to identify and contact the targeted organisations and groups of interviewees, prepare the interview instruments, and assess the effectiveness of the instruments before the entire data collection takes place.

3.5.2.1 Case Study Selection

As the purposive sample technique was used in this study, the organisations were chosen based on the functions they performed in their respective businesses. The similarities and contrasts between these organisations during the data analysis have been particularly intriguing due to the selections. It agrees with Creswell & Creswell (2018), who state that this form of selection can provide a variety of perspectives on the issues under consideration in the study.

The case study location was initially determined by evaluating a list of ministries based on information collected from the website of Bahagian Kabinet, Prime Minister's Department (2022). The organisations were then narrowed down to a final list of 12 organisations with various business functions. The case study was able to take advantage of broader viewpoints on information security governance as a result of this. Formal e-mails were sent to these organisations to seek their participation in the interview process. Seven (7) organisations responded, and only four (4), as shown in Table 3.7, consented to participate in the case study and offered access to the case study materials. As a result of a significant project they were working on, one (1) organisation withdrew their permission to participate in the case study, while the other organisation declined to participate. It was decided that all four (4) organisations would be picked based on their different core business to ensure that they were all relevant. Of the four (4) organisations chosen, two (2) are central agencies. Furthermore, the organisational contexts, such as business functions and activities, varied between the selected organisations. These cases exemplify outlier sampling in purposive sampling, in which diverse organisation operations are considered to provide particularly important information about the subject of interest and hence constitute the outlier sample in purposive sampling.

Table 3.7: List of organisations

Case	Type of Organisation	Number of Employees
Case 1	Development and human resource management	2,000
Case 2	Telecommunication and broadcasting	704
Case 3	Modernization and reformation of public sectors	950
Case 4	General administration of public sectors	500

Case 1 is an organisation responsible for the development and human resources management of the public sector in Malaysia. The number of employees is approximately 2,000. Case 1 is a central agency that holds critical information, including personal, educational, and employment of more than 1 million civil servants. The researcher interviewed eight (8) personnel for Case 1, which comprises the CIO, one (1) personnel from the information security unit, and the rest from various departments in the organisation.

The business nature of Case 2 includes providing telecommunication infrastructure, broadcasting, and the creative industry. This organisation has more than 700 employees located all over Malaysia. For Case 2, the researcher interviewed eight (8) personnel, including the CIO, four (4) from the information security field, and another three (3) participants who were not involved directly in information security work. The interview took place at the headquarters (HQ), and two (2) personnel from agencies under Case 2 agreed to come to the HQ to participate in the interview session.

Another central agency involved in the data collection was Case 3. This organisation is accountable for modernizing and transforming the public service delivery

system. More than 900 employees were working in Case 3. Initially, they were eight (8) participants accepted the interview invitation. However, only four (4) personnel were able to join. There were a few attempts to reschedule the interview session with the remaining four (4) personnel, including the CIO, but they had to refuse the interview session due to other important commitments. The CIO was replaced by one of the top management members involved directly in information security, which was a great advantage for the researcher to gain insights regarding the topic under study.

As for Case 4, there were approximately 500 employees attached to the organisation. Case 4 is responsible for managing public service members' appointments, termination, and disciplinary action. The CIO, four (4) personnel from the information security unit and two (2) personnel from other departments in the organisation agreed to participate in the data collection at the HQ.

According to Zucker (2002), in the policy of the *Archives of Sexual Behavior* cited by Dworkin (2012), it is recommended that a sample size of 25-30 people be used when conducting in-depth interviews. This sample size is sufficient because it increases the likelihood that enough data have been collected to clarify relationships between conceptual categories and identify variation in processes, increases the likelihood that negative cases and hypothetical negative cases have been explored in the data, and minimises the likelihood that insufficient data have been collected (Charmaz, 2006; Morse, 2000). For this study, the researcher stopped the interview when it reached 27 participants when the researcher observed that the data input had reached saturation. That means no additional data from other candidates could provide new insights into the research, and the interview was terminated (Creswell & Creswell, 2018; Dworkin, 2012). Therefore, the researcher is of the view that the sampling size of 27 is adequate for this research.

3.5.2.2 Access Strategy

A flexible strategy or action plan is needed to acquire access to the organisations where the case studies are done (Djamba & Neuman, 2002). Researchers need to have a suitable strategy to ensure that they do not experience challenges while collecting data from organisations and do not acquire shallow or unrelated data to their study objectives. In order to get entry into an organisation, research methodologies and roles adopted by researchers must be taken into account (Gummesson, 2000). When it came to acquiring access to the organisations, the role of an academic researcher was chosen. Furthermore, the researcher identified herself as a civil servant in one of the ministries, which increased the likelihood of trust being established.

The first stage in developing an access strategy is getting a confirmation letter and notifying the data collection organisation of the intention to gather data. The letters were received from the Deputy Dean of Postgraduate and Research at the International Islamic University Malaysia (IIUM), the institution where the researcher is pursuing a doctoral degree. In order to obtain proper authorization for data collection, the letter was attached along with a study synopsis and project description from the institution, which were addressed to the CIO. The researcher decided to gain permission from the CIO because the researcher believes that permission from someone who has a high rank in information security and a member of top management like the CIO would make accessing the case site easier. It is proven that more than half of the organisations responded out of the twelve organisations that the researcher contacted, mainly through the CIO. All CIOs agreed to participate in the data collection and also proposed the name of the “gatekeeper” for follow-ups.

"Gatekeepers" have the authority to allow or deny access to the researcher, informants, and individuals who can supply vital information and smooth the path for others (Gummesson, 2000). These "gatekeepers" ensure that the researcher can access the organisation’s resources adequately. The "gatekeeper" was critical in ensuring that the data-

gathering sessions ran smoothly and successfully. The researcher then provided the "gatekeepers" with the criteria for interview participants, which included the planned number of participants per organisation once the researcher was authorised to access. The researcher also requested that the participants be from three levels of designation: the CIO or top management, information security personnel (members of the organisation who work directly in the information security unit or team), and personnel who do not work in the information security field (other members of the organisation), as depicted in Table 3.8. These criteria allow the study to get rich input from *multiple perspectives* of the participants and organisations. The "gatekeeper" from each organisation gave excellent cooperation and commitment by preparing the interview schedule. The researcher managed to have a dedicated room and was allocated around one to two hours of interview slots for every 27 participants for the interview session. The researcher was also allowed to do document review and observation in all four (4) organisations despite the busy schedule of each participant.

Approval from the CIO to participate in the data collection and instructions from the CIO is believed to be one of the reasons that the researcher did not face any significant difficulty accessing the case site. Furthermore, each respondent was promised confidentiality by signing the consent form during each interview session. Due to this, each participant felt confident, transparent and honest in providing views and answering each interview question and agreed for the interview to be audio recorded. Table 3.8 shows the total number of participants for each case, and the full details, including pseudocode, are listed in Appendix N.

Table 3.8: List of case and participant

Case	Number of Participants			Total
	CIO/Top Management	Information Security Personnel	Non-Information Security Personnel	
Case 1 *(A1)*	**1** *(A1TM1)*	**1** *(A1IS1)*	**6** *(A1NIS1)* *(A1NIS2)* *(A1NIS3)* *(A1NIS4)* *(A1NIS5)* *(A1NIS6)*	8
Case 2 *(A2)*	**1** *(A2TM1)*	**4** *(A2IS1)* *(A2IS2)* *(A2IS3)* *(A2IS4)*	**3** *(A2NIS1)* *(A2NIS2)* *(A2NIS3)*	8
Case 3 *(A3)*	**1** *(A3TM1)*	**2** *(A3IS1)* *(A3IS2)*	**1** *(A3NIS1)*	4
Case 4 *(A4)*	**1** *(A4TM1)*	**4** *(A4IS1)* *(A4IS2)* *(A4IS3)* *(A4IS4)*	**2** *(A4NIS1)* *(A4NIS2)*	7
			GRAND TOTAL	**27**

3.5.2.3 Data Collection Instruments

Several items were utilised as instruments throughout the study's data gathering. Table 3.9 represents all the research instruments used during the data collection.

Table 3.9: Research instruments

Instrument	**Usage**
Case study protocol *(Appendix A)*	To outline the procedure and general guidelines for performing the case study, as well as a summary of the data that will be collected in the field
Confirmation letter *(Appendix B)*	A letter was obtained from the university to confirm that the researcher is a student and in the process of collecting data at the organisations
Consent form *(Appendix C)*	A consent form for the person participating in the research to acknowledge that the interview session is joined voluntarily, all information given is kept confidential, and agree to be audio recorded
Interview checklist *(Appendix D)*	A thing-to-do checklist as a guide for the researcher to ensure the researcher does all the necessary actions before, prior, and after the interview session
Demographic survey form *(Appendix E)*	A form to be filled up by the participant before the interview session which consists of his/her basic information background, i.e. name, approximate age, tenure in the organisation, education background, his/her role in the organisation, basic knowledge regarding information security policy in his/her organisation. This form is also be used to determine which set of interview questions to be asked to the participant

Instrument	**Usage**
Interview questions *(Appendix F)*	List of questions to be asked to the participants during the interview session
Contact summary form *(Appendix G)* *(Adopted from Rahim (2009))*	To jot down interview points and the summary of the interview
Observation checklist *(Appendix H)* *(Adopted from Rahim (2009))*	Observation checklist to be done at the organisation
Document review form *(Appendix I)* *(Adopted from Rahim (2009))*	To jot down document review points and the summary of the document
Research Description *(Appendix J)*	A research project description was sent to organisations as an attachment to the e-mail invitation to participate. This document gives an overview of what participants need to know and expect to do prior to the interview session
Research Summary *(Appendix K)*	A project summary was sent to organisations as an attachment to the e-mail invitation to participate. This document provides a summary of the research
Voice recorder	To record the audio of the interview

The case study protocol is not just an instrument but also a critical guide for the researchers in performing the study and increasing the research's reliability (Yin, 2018). On the other hand, the contact and document summary forms are critical tools for recording and summarising field contacts and documents under review (Miles et al., 2014). The researcher took the initiative to prepare an interview checklist to ensure not to miss the

essential things to do while collecting data at the site. A confirmation letter from the university and the consent form is vital to establish trust among the participants. Therefore, participants feel confident that every input shared with the researcher would not reveal their true identity and be presented using pseudonyms.

Meanwhile, the demographic survey was created to collect basic participants' information and awareness of the information security policy in their organisation. It also aims to determine the set of questions to be asked during the interview based on the participant's role in the organisation. The survey also saves interview time as participants have already filled up these basic matters. The survey fill-up session before the interview also allows researchers to prepare the instruments for the interview session (turn on the audio recorder, prepare forms, stationery, etc.) while waiting for participants to complete the survey and avoid awkward situations before the interview.

3.5.2.4 Mock Interviews

The developed initial research model in Phase I was used as a guideline to build interview questions. The interview questions were intended to be consistent across all three designation levels, namely as CIO/top management, information security personnel, and non-information security personnel, to ensure that all questions are uniform throughout all three designation levels. However, additional questions and adaptations are made in accordance with the circumstances of the designation. Each question was also carefully designed to cover all aspects of the research objectives.

The interview questions were subjected to multiple rounds of testing in a session dubbed "mock interviews" before finalising. This testing procedure is in place to guarantee that the questions are appropriate for investigating the phenomenon. The researcher consulted lecturers, graduate students in the faculty where the researcher is pursuing doctorate study, and acquaintances from both the public and private sectors about their

experiences in the mock interviews. The selection of respondents from different employment and educational backgrounds ensures that they understand the questions posed. A total of eight (8) mock interviews were conducted through convenience sampling. The participants during the mock interviews are as in Table 3.10.

Table 3.10: Participants for mock interviews

Pseudonym	**Role**	**Sector**	**Work or study in the information security field?**
M1	Lecturer	Private	No
M2	Part-time postgraduate student	Private	No
M3	Full-time postgraduate student	-	Yes
M4	Full-time postgraduate student	-	No
M5	Full-time postgraduate student	Public	No
M6	Full-time postgraduate student	-	No
M7	IT Officer	Public	Yes
M8	Executive	Private	Yes

During the mock interviews, the goal is to refine the initial interview questions and make them understandable to technical people and people who are not technically oriented. Mock interviews also served as a practice ground for data collection, allowing participants to become familiar with the instruments before the actual data collection at the sites.

Through mock interviews, it is possible to evaluate the instrument in order to verify the consistency and soundness of the data collection instruments. The researcher considered several elements: the respondents' understanding of the questions posed, the continuity between one question to another, and the expected interview duration for each respondent. After considering all the comments and suggestions each respondent gave, the interview questions' draft was improved and then brought into a discussion session with the supervisors and research committee for approval. Then only the question is ready for use in the actual interview session. Experience gained from the mock interviews may be used to build strategies for doing better exploration during the actual data collection.

3.5.3 Phase III: Field Investigation

There were two phases to the data collection process. A total of ten (10) weeks were spent collecting data. Six (6) weeks were required to conduct 27 semi-structured interviews, with the longest session lasting approximately one (1) hour, 32 minutes, and 51 seconds. In contrast, the shortest interview session lasted roughly 21 minutes and 41 seconds (see Appendix N). It included multiple phone calls, e-mails, and informal meetings, including online meetings, with respondents in order to obtain additional information and confirm the information provided. Each respondent consented to be audio-recorded throughout the duration of the interview, so the researcher had no problems recording it. Before the interview, the researcher distributed questionnaires (see Appendix E) to collect demographic information from the respondents.

The second phase of data collection, which took approximately four (4) weeks, included follow-up calls and reminder emails given to participants who could not participate in the first interview session due to unforeseen circumstances. In addition, during this second phase, follow-ups were conducted with participants who had previously stated that they would give further information and materials during the first phase of the

interviews. The participants involved in the interview session were categorised into three (3) levels, as mentioned in Table 3.8.

During the field investigation, sources of evidence are a set of facts or opinions that can draw meaning from a subject to understand the phenomenon. It is either for reference or analysis purposes (Saunders et al., 2016). According to Yin (2018), case studies can gain evidence from six (6) primary sources, requiring different data collection procedures. The six (6) primary sources are archival records, documentation, participant observation, direct observations, interviews, and physical artefacts. For this study, the researcher adopted three (3) sources of evidence as follows:

3.5.3.1 Source of Evidence 1: Interview

Interviews were conducted on a one-to-one basis to get in-depth insight and interpretations about phenomena, events, people, opinions, explanations, or meanings of a particular event from the key informants (Yin, 2018). This study implemented the interview technique via semi-structured questions, allowing better data coverage. Even though the open-ended questions are better as the participants are able to express everything (Creswell & Creswell, 2018), a semi-structured interview was chosen to minimize distraction to the researcher and participants based on the guided questions. It allows the researcher to control the interview session and avoid straying too far from the discussed topics. Even though several key questions guided the interviews, semi-structured interviews would not refrain the researcher and participant from asking and responding in more detail.

Although this interview used a semi-structured approach, several participants in each agency made this interview session a place to express dissatisfaction with their work, organisation, and top management. The researcher had to be meticulous in dealing with this situation because it was feared that this session would take too long while many questions still needed to be answered. However, the semi-structured approach helped researchers deal

with these kinds of situations. Sometimes participants had facts that could be used to provide significant input for the study that the researcher had never thought of before. However, if the session ran too long and was irrelevant, the researcher would gently pull the participants back into the interview context.

There were times when the researcher had to push the participants to provide additional information based on their first responses, summarise their responses in order to obtain clarification, or explore deeper into their responses. All the interviews were conducted mainly in the Malay Language with a combination of English. Since Malay Language is the official language of the Malaysian government, it is widely spoken by public officials in the areas where the case studies were conducted. Each interview lasted from half an hour to a hundred and twenty minutes in duration. Since the interviews took place during office hours and some of the participants were among the top-level management, time became the major constraint since they were busy and occupied with their jobs and responsibilities. The interviews were all audio-recorded with the consent of the participants and then transcribed verbatim from the recordings. The recording is to ensure that rich qualitative data was recorded and, simultaneously, participants' confidentiality was addressed. After completing the transcription process, the transcripts were submitted to the participants for review. It is to confirm that the interview details had caught the intended meaning of the participants. Following that, the transcripts were revised if needed and filed in the proper order.

Overall, researchers received excellent cooperation from all four (4) organisations. From CIO to Gatekeeper and all the interview participants provided strong support for this data collection activities. The cooperation gained from all organisations made this session a breeze, and it did not take long to obtain permission for interviews.

3.5.3.2 Source of Evidence 2: Observation

Direct observation is to witness what is happening in the real world related to an environment or phenomena relevant to this study in particular periods (Yin, 2018). This study applied the observation technique in two (2) ways. First, general observation was conducted where information security is practised in the organisations, and it includes the observation of how employees embed the information security culture in their workplace. Even though this observation seemed simple, it is significant and gives an impression that the awareness regarding their information security policy among members of the organisation is communicated. Waiting and breaks in between appointments allowed the researcher to study the ambience and surroundings of each department in the organisation. This exercise includes watching, listening, and taking notes on what is going on concerning an organisation's information security daily practice.

Second, observation was conducted during interviews with the participants. The observation considered their facial expression, body language and the way they answered the interview questions. For instance, when the participants knit their eyebrows, there is a possibility that they do not understand the question. Therefore, it became the responsibility of the researcher to repeat the question or give further explanations more straightforwardly. However, there was no intention to incorporate video recording for this purpose. At the end of the observation session, the notes taken were adequately arranged for further analysis.

3.5.3.3 Source of Evidence 3: Document Review

Documented information is essential in collecting data for the case study as it provides specific and comprehensive information, and the information is reviewable when needed (Stake, 2006; Yin, 2018). It is available in paper or electronic form can be used in every case study, and can capture missing information from the interviews and observations (Cresswell, 2014). Among the documents to be reviewed were security policy, documents,

records and images for information security initiatives, government circulars, organisations' information security decisions, or published materials regarding information security in the organisations. Any information gathered about the information security programs was analysed as well. The documents are listed in Section 3.6.

3.5.4 Phase IV: Thematic and Single-Case Analysis

The analysis phase is crucial and inevitable in the research cycle, regardless of the methodology adopted. In contrast with quantitative research, qualitative data analysis has less well-established and commonly acknowledged norms and guidelines (Sekaran & Bougie, 2016). However, some general approaches to qualitative data analysis have emerged over time (Creswell & Creswell, 2018; Miles et al., 2014; Sekaran & Bougie, 2016). Miles et al. (2014) suggest that qualitative data analysis consists of three (3) steps; data reduction, data display, and drawing conclusions. These steps were adopted by the researcher when performing thematic analysis.

3.5.4.1 Step 1: Data Reduction

Large amounts of data are generated during qualitative data collection, including the recorded interviews, observation notes, and documents review. The 27 recorded interviews were manually transcribed verbatim into 486 pages of a text document, where the average page for each participant is 18. The researcher repeatedly read the interview transcripts to refresh and familiarize herself with the data before taking the following actions.

Later, data was reduced through coding and categorization. According to Miles et al. (2014) and Sekaran & Bougie (2016), coding is the analytic process of reducing, rearranging, and integrating qualitative data to generate theory. Through coding, meaningful data can be generated, and these codes are grouped to produce Categories.

Categorization is the process of arranging, grouping and categorizing code elements (Sekaran & Bougie, 2016). Inductive and deductive approaches can be used to create codes and categories. Using a deductive technique, the researcher develops codes and categories based on the preliminary theory identified in Phase I. For the study, an initial list of codes and categories is retrieved from the theory and the literature reviews, and as long as the analysis is taking place, other codes and categories can be derived inductively (Miles et al., 2014) and expand the knowledge as the analysis progress.

This coding and categorizing process is not a one-off action but rather an iterative process where it is often revisited to understand the data better, create the link, identify the pattern, and organize as the new connections are discovered (Miles et al., 2014; Sekaran & Bougie, 2016). The researcher used the data analysis software Atlas.ti version 22.0 to code and categorise. The researcher also used Microsoft Excel interchangeably, as Atlas.ti data can also be exported to Microsoft Excel for further analysis.

Generally, the next stage is single-case analysis after deriving the theme and sub-themes from the data. Data from three (3) designation levels were analysed within the case. After completing the study of all single cases, the researcher moved on to the next phase, which is the cross-case analysis, before a conclusion can be made. The single-case and cross-case analysis is illustrated in Figure 3.3.

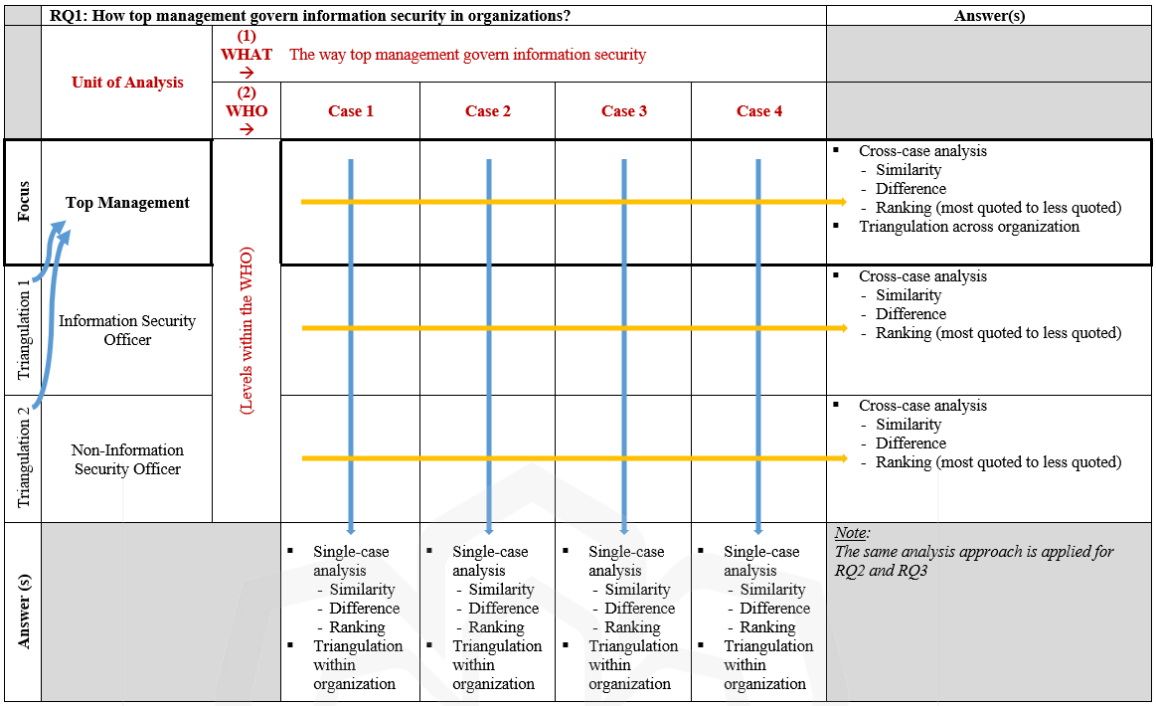


Figure 3.3: Analysis approach involving single-case and cross-case

3.5.4.2 Step 2: Data Display

When conducting qualitative research, data display, according to Miles et al. (2014), is the second important activity that researchers should engage in after data collection. Data display means taking the reduced data and presenting it in an organized and concise manner and presenting it through charts, matrixes, diagrams, graphs, and other illustration diagrams or tools. It assists researchers in organizing data, discovering patterns and links in the data, and drawing conclusions easier (Miles et al., 2014; Sekaran & Bougie, 2016).

A matrix using Microsoft Excel was considered the primary display for the study to bring together the qualitative data. Cells were indicated with multi-colours for better visibility. Other than that, linkage and network between the data were generated using Atlas.ti for a more graphical look. The matrix of data is presented and discussed extensively in Chapter Four.

3.5.4.3 Step 3: Drawing Conclusions

Following Miles et al. (2014), drawing conclusions is the final step in qualitative data analysis and the most critical step in data analysis. At this point, the themes that have been identified provide answers to the study questions, patterns and linkages have been identified, and contrasts and comparisons have been drawn (Miles et al., 2014; Sekaran & Bougie, 2016). The essence of this step is heavily discussed in Chapter Five.

3.5.5 Phase IV: Cross-Case Analysis and Conclusion

The data from each case was analysed separately before a cross-case analysis was carried out. A cross-case analysis was done to draw attention to the differences and similarities between all four (4) cases. The cross-case study generates insights that the single-case analysis is lacking. It also yields findings that may be generalizable to all cases, depending on the circumstances. However, the study is not designed to produce generalizations. The generalisations drawn from qualitative research are typically limited to a particular time, investigation's breadth, and research context. The findings of the study, on the other hand, might be useful for future quantitative research that can be tested on a bigger sample size and could be generalised to a larger population. It is possible to draw a conclusion about the understanding of top management engagement in governing information security based on the results of the cross-case analysis and the other analysis performed throughout the study. The initial research model is revisited and refined based on the findings gained from the field investigation.

3.6 RELIABILITY AND VALIDITY OF QUALITATIVE DATA

In qualitative research, reliability and validity have somewhat different meanings than in quantitative research. The reliability of a measure does not have any bias, errors, or flaws,

which means that it can be used over time to measure different things in the same way (Miles et al., 2014; Sekaran & Bougie, 2016). Both scholars also argue that the reliability of a measure indicates how stable and consistent the instrument is when it comes to measuring a concept.

According to Yin (2018), qualitative researchers should record their case study procedures in as much detail as possible. For the benefit of future researchers, it is suggested to document and archive meticulous case study protocols and data. Therefore, in order to ensure the reliability and validity of this study, the researcher has provided instruments and implemented procedures that can balance bias and errors in studies, including:

(a) Check the validity of the initial research model. The multiple-case study adopted by this research is used as *part of validating the initial research model* developed in Chapter Two. Establishing an initial research model provides multiple perspectives for a more in-depth understanding of the factors that influence the participation and involvement of top management in information security initiatives derived from the past literature. Then, the viability of the initial research model is demonstrated by its application in conducting the field investigation of actual case studies. Findings from the case studies provided evidence of the initial research model, particularly the factors influencing top management engagement in information security. The process of validating the model includes alterations and modifications to the initial research model based on the findings and evidence from the multiple-case studies. As a result, the initial research model becomes a qualitative validated model. In this research, a multiple-case study is employed as part of the procedure for validating the initial model.

(b) Check the validity and accuracy by triangulating multiple sources to provide a solid rationale for the findings (themes). The researcher reviewed government documents, including official websites, to check the accuracy of the findings.

This list of important documents includes, but is not limited to, the following items:

i. Public Sector's Cyber Security Framework, version 1.0;
ii. Information Technology Security and Communication Framework (Bil. 3/2000);
iii. Malaysia Cyber Security Strategy 2020-2024;
iv. Instruction Letter for the implementation of MS ISO/IEC 27001 ISMS Certification in public sectors;
v. MAMPU's Cyber Security Policy;
vi. Information Security Policies of all case studies;
vii. Letter for ICTSO's public sector information management from National Security Council to all government agencies; and
viii. Other related documented information, i.e. ISO/IEC 27000 standard documents

(c) Check the validity and accuracy by interviewing three (3) levels of participants for each case; top management, information security officer, and non-information security officer. This is to produce multiple perspectives of data gathering from different levels of organisation members. The researcher also observes the field environment to see whether information security practices align with the claims made by the participants.

(d) Check the reliability by setting up a detailed case study protocol (Appendix A). The case study protocol is not only an instrument, but it also serves as an essential guide for the researchers to follow in order to carry out the case study successfully and to ensure the reliability of the study (Yin, 2018). Therefore, this case protocol is used as a guideline for the research to conduct data collection in all case studies.

(e) According to Miles et al. (2014), a contact and document summary form is useful for recording and summarising information about interactions in the field and the documents under review. Therefore, the researcher developed and used other research instruments, such as an interview checklist (Appendix D), a

demographic survey form (Appendix E), an observation checklist (Appendix H), and a document review form (Appendix J), to record all findings during the field investigation. All research instruments are listed in Table 3.9.

(f) During the analysis phase, the researcher revised interview transcriptions frequently to check for mistakes during transcription. The researcher also conducted a session to cross-check codes with two (2) external coders to ensure all codes are coherent and yield consistent results. Several steps are involved in this reliability procedure, which is explained in detail in the next section.

3.6.1 Measuring Reliability of Codes

Qualitative data analysis measures include category and interjudge reliability (Kassarjian, 1977; Sekaran & Bougie, 2016). Kassarjian (1977, p.14) defined category reliability as "depends on the analyst's ability to formulate categories and present to competent judges definitions of the categories, so they will agree on which items of a certain population belong in a category and which do not". It means category reliability refers to the extent to which judges can categorise qualitative data using category definitions. Well-defined categories result in increased category reliability (Kassarjian, 1977; Sekaran & Bougie, 2016). Meanwhile, interjudge reliability is a measure of consistency amongst coders working with the same data (Creswell & Creswell, 2018; Kassarjian, 1977; Sekaran & Bougie, 2016). The percentage of coding agreements relative to the total number of coding judgments is commonly used to indicate interjudge reliability (Sekaran & Bougie, 2016).

In order to measure the reliability of the study, the researcher applied interjudge reliability to examine the code agreement between raters. Even though the reliability in qualitative research is difficult to quantify since the nature of qualitative research is flexible and subjective, the reliability of coding qualitative research data could be improved by using a reliability measurement approaches such as Cohen's Kappa, which is known as inter-coder reliability or inter-rater reliability (Othman Talib, 2018). Inter-coder reliability

is used to examine the agreement between two (2) raters or observers on the assignment of categories of a categorical variable. It is an important measure in determining how well the implementation of some coding or measurement system works (Othman Talib, 2018).

Researchers in many areas have grown more conscious of the importance of the raters or observers as a significant source of measurement error in their studies (Landis & Koch, 1977). There are many approaches to measure reliability, for instance, Cohen's Kappa, Scott's Pi, Fleiss' Kappa, and Krippendorff's Alpha, to name a few. The researcher chooses Cohen's Kappa approach for the study to determine consistency between two (2) coders in processing data, in this case, coding the interview transcripts. There were some steps involved in measuring the reliability as described by Talib (2018) as follows:

(a) Step 1: Prepare interview transcripts
(b) Step 2: Prepare a coding schema
(c) Step 3: Appoint at least two individuals who are experts in coding to code the transcripts based on schema
(d) Step 4: Record coding results from the experts
(e) Step 5: Use statistical analysis software to calculate the coding results

The researcher appointed two (2) experts to assist in measuring the coding transcripts' reliability. A list containing ten (10) quotations and a selection of codes were distributed to the experts. After the experts had completed answering, the coding session outputs were keyed into analysis software called SPSS Statistics. Figure 3.4 shows the agreement measures using Cohen's Kappa approach.

AGREEMENT MEASURES FOR CATEGORICAL DATA

Kappa Statistic	*Strength of Agreement*
<0.00	Poor
0.00–0.20	Slight
0.21–0.40	Fair
0.41–0.60	Moderate
0.61–0.80	Substantial
0.81–1.00	Almost Perfect

Figure 3.4: The Cohen's Kappa agreement measures for categorical data

The SPSS Statistics generated the result, and the inter-coder reliability for the coders was found to be **Kappa = 0.78,** as depicted in Figure 3.5. The result indicates a *Substantial* agreement between the coders. Meaning to say, the researcher's transcript codes were consistent and had a high rate of agreement among the coders, thus reliable.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Coder 1 * Coder 2	10	100.0%	0	0.0%	10	100.0%

Coder 1 * Coder 2 Crosstabulation

Count

		Coder 2										
		A	B	C	D	E	F	G	H	I	J	Total
Coder 1	A	1	0	0	0	0	0	0	0	0	0	1
	B	0	1	0	0	0	0	0	0	0	0	1
	C	0	0	1	0	0	0	0	0	0	0	1
	D	0	0	0	1	0	0	0	0	0	0	1
	E	0	0	0	0	1	0	0	0	0	0	1
	F	0	0	0	0	0	0	0	1	0	0	1
	G	0	0	0	0	0	0	1	0	0	0	1
	H	0	0	0	0	0	1	0	0	0	0	1
	I	0	0	0	0	0	0	0	0	1	0	1
	J	0	0	0	0	0	0	0	0	0	1	1
Total		1	1	1	1	1	1	1	1	1	1	10

Symmetric Measures

		Value	Asymptotic Standard Error [a]	Approximate T[b]	Approximate Significance
Measure of Agreement	Kappa	.778	.141	7.379	<.001
N of Valid Cases		10			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

Figure 3.5: Result from the SPSS statistics software for inter-coder reliability measurement

3.7 THE ROLE OF THE RESEARCHER

As Creswell & Creswell (2018) and Yin (2018) have pointed out, data collection and analysis rely heavily on the researcher. The researcher plays a pivotal role in qualitative research by constructing an intricate and comprehensive picture, analysing the data, and reporting the results (Creswell & Creswell, 2018). However, many safeguards against errors afforded by statistical methods or standardised measures are unavailable to qualitative researchers. In other words, it depends on their knowledge, faith, honesty, and integrity while conducting research. Therefore, it makes the researcher's position less protected from criticism.

The one-on-one nature of the interview makes it susceptible to bias; therefore, the researcher has followed all of the guidelines outlined in the case study protocol to ensure the accuracy of the data. The selected case studies are not a ministry or organisation for which the researcher works or has served. The Gatekeeper also selected interview participants from each case study based on some of the basic criteria established by the researcher. The Gatekeeper also determines the interview time, except for some interview sessions that must be rescheduled because participants have other obligations during the interview.

During the data collection session, the researcher recorded all findings using the research instrument, which included an audio recorder. For instance, an interview checklist is utilised to ensure all necessary steps are completed before, during, and after the interview. The demographic form was provided to the participant before the interview session to provide their basic information to avoid wasting time. The researcher relies solely on semi-structured interview questions during the interview session. Although the questions have been prepared in advance, participants are free to express their opinions based on the questions posed without the researcher engaging in a social conversation with them or sharing the researcher's experiences, which could influence how they respond to the questions. The researcher was impartial and unbiased, allowing all participants to explain the specifics. Each interview, observation, and document review finding is recorded immediately on each summary form. For verification purposes, claims made by participants were triangulated with official government documents. Since this study involved the participation of top management in information security, the participant not only from top management, but the researcher also interviewed information security personnel and non-information security personnel to obtain a broader, less biased perspective. It is consistent with the concept introduced by the MPC, which was used as a baseline for constructing the initial research model for this study, in which multiple perspectives data were gathered based on external, organisational, and personal components.

To perform the analysis of collected data, the researcher attended six (6) training including workshop sessions organised on and off campus. The training and workshop sessions comprise data collection for a qualitative researcher using Atlas.ti analysis software, and guidelines for producing code and theme for thematic analysis. As part of the implementation of the coding process for the interview transcription, the existing codes were reviewed during the cross-check codes session to ensure code consistency. This process is outlined in detail in Section 3.6.1. In addition, the research methodology and data analysis processes have been described in Chapter Three and Four, respectively.

3.8 CHAPTER SUMMARY

This chapter describes the research methodology used to guide the study to achieve its objectives. It started with Research Paradigm (Section 3.2) that elaborated on the ontological and epistemological concerning positivist and interpretive paradigms. The researcher decided to adopt interpretive paradigms as it is deemed suitable to explain the top management engagement in information security within Malaysian public sectors. The discussion continues with the Research Approach (Section 3.3), where the researcher chose the qualitative methodological approach and multiple-case study as the Research Strategy and also as part of the process of validating the initial research model of the study (Section 3.4). This section also explains the unit of analysis and sampling techniques where the researcher used embedded design and purposive sampling, respectively. Moving to the next section, which is Research Design (Section 3.5), the researcher explicitly explained the five (5) significant phases of collecting data; starting from the preparation, during the field investigation of four (4) cases, analysis phase after the data collection, until a conclusion is drawn from the study. Reliability of Qualitative Data (Section 3.6) reported how reliability measurement was conducted between two (2) coders, and the result derived from Cohen's Kappa approach. Finally, the role of the researcher is explained, as it is essential to avoid bias and errors in conducting research (Section 3.7).

CHAPTER FOUR

DATA ANALYSIS AND RESEARCH FINDINGS

4.1 OVERVIEW

After the interview, the analysis process is done to produce useful information to answer the research questions. This chapter discusses the analysis of the data, a list of themes and sub-themes, research findings and emerging findings. All sections are arranged as in Figure 4.1.

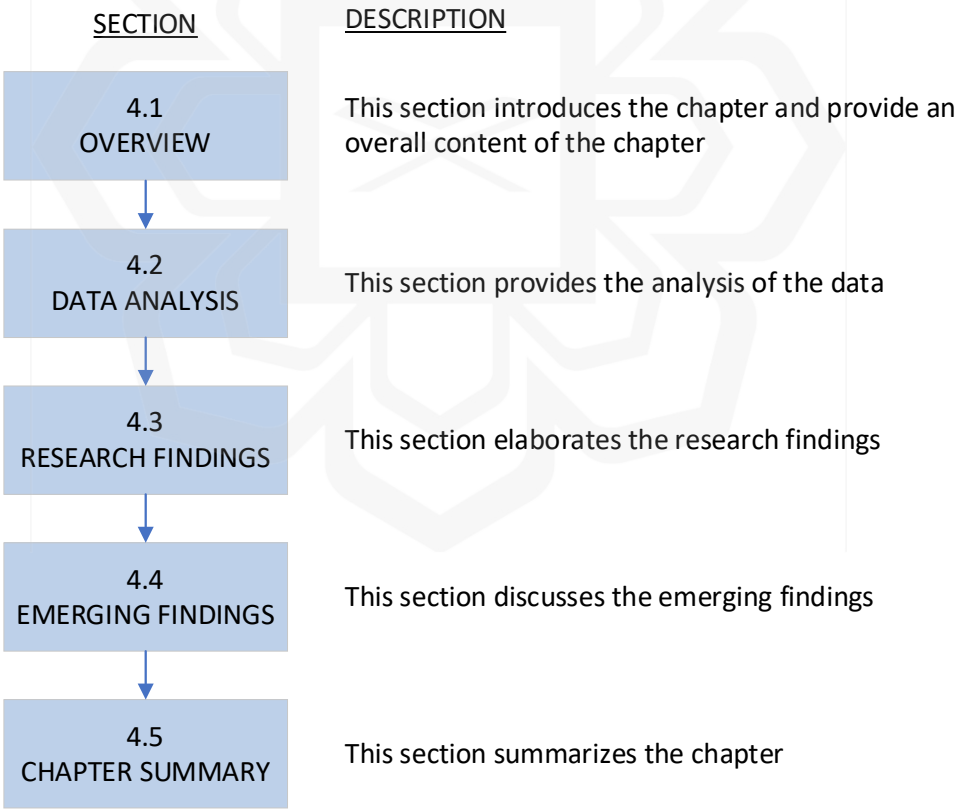


Figure 4.1: Organisation of Chapter Four

4.2 DATA ANALYSIS

Every audio-recorded interview was transcribed verbatim. Due to the lengthy interview sessions, the researcher required approximately 20 weeks to transcribe the data. As stated in Section 3.5.4.1, the total number of interview transcripts was 486 pages, with an average of 18 pages per participant (see Appendix N). Each transcript was presented to respondents in person to ensure their confidentiality and authenticity and fulfil their meaning.

Once the transcript verification process is completed, a thorough analysis of the transcripts is done using a thematic analysis approach. Each transcript was read repeatedly, line by line, to understand and familiarize the entire interview transcripts and what is equivalent to what the respondent conveyed. Because of so much input in each transcript, research objectives are often referred to in order to prevent the researcher from drowning in data and slipping behind the study's goal. With the help of Atlas.ti software, codes are extracted from each transcript. For coding purposes, the researcher adapted three (3) coding types used in grounded theory research: open coding, axial coding, and selective coding, as proposed by Corbin & Strauss (1990). The analysis process is illustrated as in Figure 4.2.

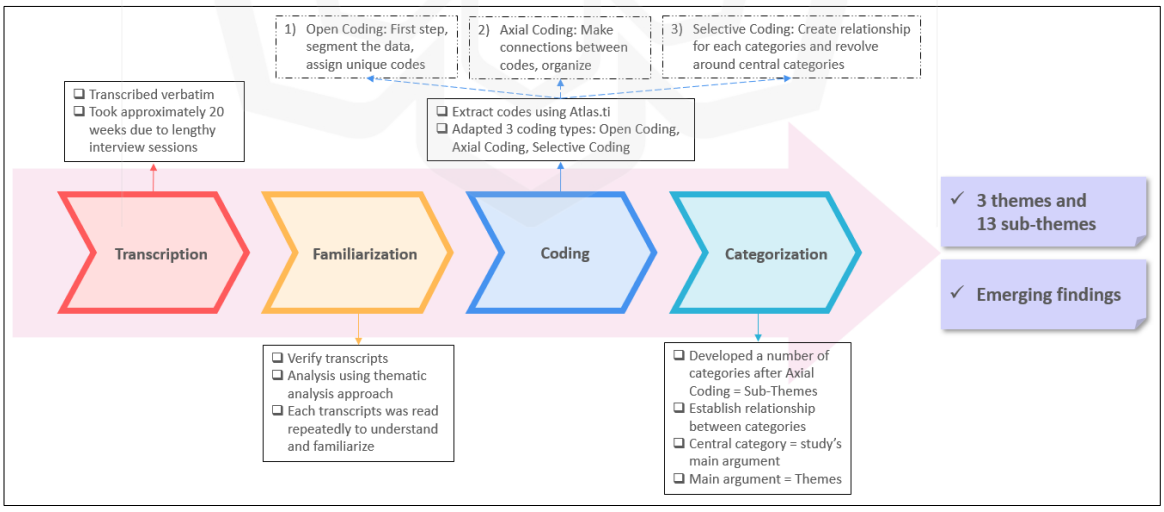


Figure 4.2: The analysis process

Open coding is a common first step in the analysis process when conducting a grounded theory study or some other kind of qualitative research (Corbin & Strauss, 1990). The data is segmented, and the researcher assigns unique codes to each segment. The researcher then repeatedly looks for patterns in the data and compares them. In doing so, the researcher is able to keep any biases or assumptions about the researcher's research.

Following the completion of the open coding phase, axial coding was implemented. In axial coding, researchers begin to make connections between codes to organise the codes developed in open coding, as opposed to open coding's focus on breaking data into discrete parts. A thorough analysis of all codes and supporting data allowed the researcher to identify commonalities between them. The researcher began to develop a number of categories after using axial coding, and these categories now have a more refined set of supporting codes to back them up. These categories became the Sub-Theme for this study.

Finalizing a grounded theory with selective coding involves establishing relationships between categories that revolve around a central category. By doing so, the researcher established a single overarching theory to guide the study. The central category stands for the study's main argument. For this study, the central categories became the Themes, and these themes satisfy each research question. There were also findings which have not been mentioned in the literature but emerged during the analysis phase and were coded to become the emerging findings.

The steps explained in previous paragraphs where data is familiarised, coded, and categorised were the processes involved in *Data Reduction*, *Data Display,* and *Drawing Conclusions* adapted by this study which was mentioned in Section 3.5.4.1, 3.5.4.2 and 3.5.4.3, respectively. This thematic analysis is an adaptable and valuable research tool that has the potential to reveal a comprehensive and intricate picture of the data. It is important to recognise the role of thematic analysis as a cornerstone of qualitative research (Braun & Clarke, 2006).

As a result of the analysis of all interview transcripts, three (3) themes and 13 sub-themes were derived, including the emerging findings. The themes and sub-themes address each research question, as presented in Table 4.1, and the definition of each sub-themes is presented in Table 4.2.

Table 4.1: Themes and sub-themes discovered from data collection

No	Theme	Sub-Theme	
1	Information Security Governance Approach *(Address Research Question 1)*	Top management leadership style in governing information security	▪ Laissez-Faire (bottom-up)
			▪ Authoritarian (top-down)
			▪ Democratic (both ways)
		Platform to discuss information security	▪ Top management meeting
			▪ Steering Committee for ICT and Security (JPICT)
			▪ Committee for ISMS
		Top management practices in governing information security	▪ Compliance to the public sector's information security direction
			▪ Communication of information security awareness and initiative
			▪ Enforcement against information security misconduct
		Information security budget	▪ The approved information security budget
			▪ Case-based budget approval
		Employee competency development in information security	▪ Training for information security employees
			▪ Information security awareness to all employees

No	Theme	Sub-Theme	
		Monitoring of information security implementation	▪ Presentation by the information security team in meeting/audit meeting
			▪ Establishment of committee
			▪ Information security reports or meeting minutes submitted to top management
2	Factors Influencing Top Management Engagement in Information Security *(Address Research Question 2)*	External factor	▪ Regulatory forces
			▪ Imitating good practice
			▪ Changes in security risk exposure
			▪ Audit compliance
		Organisational factor	▪ Reputation
			▪ Information security risk awareness
			▪ Information security committee structure
			▪ Culture
		Personal factor	▪ Informal education
			▪ On-the-job exposure
			▪ Formal education
3	Information Security Governance Issues	Top management constraint	▪ Limited bandwidth due to hectic schedule and various meeting agenda

No	Theme	Sub-Theme	
	(Address Research Question 3)		▪ Inadequate knowledge and experience in information security
			▪ Reactive in handling information security issues
			▪ Information security is not an integral part of the organisation's business
			▪ Generation gap of top management
		Resource constraint	▪ Insufficient budget allocation
			▪ Insufficient human capital
		Challenges in employee acceptance of information security	▪ Difficult to control staff
			▪ Employee lack of information security awareness
		Organisation's culture	▪ Focus only on passing audit compliance
			▪ The misconception of information security and ownership
			▪ Difficult to change job routines

Based on Table 4.1, one (1) theme and six (6) sub-themes address the first research question. These themes and sub-themes refer to how top management in public sector organisations administers and leads information security initiatives. The second research question is represented by one (1) theme and three (3) sub-themes that show the factors influencing top management's engagement in information security within their organisation. For the third research question, one (1) theme and four (4) sub-themes address the issues faced by top management and the organisation in administering and undertaking information security initiatives in public sector organisations. The definition of each sub-themes is presented in Table 4.2.

Table 4.2: The description of each sub-themes

No	Theme	Sub-Theme		Description
1	Information Security Governance Approach *(Address Research Question 1)*	Top management leadership style in governing information security	Laissez-Faire *(bottom-up)*	The direction of information security is an initiative from the bottom up. Top management delegated complete information security duties to the information security team. Rather than accepting instructions and executing, the information security team is self-directed and thinks of the best approach to do each assignment. The team is responsible for offering management high-level advice, proposals, and implementation. The recommended information security actions are being reviewed by high management.
			Authoritarian *(top-down)*	The direction of information security is determined by top management. The authority for such directions comes from external sources such as the prime minister's speech, information security agencies circulars, or reports from information security devices. Typically, the instructions are communicated to the information security team and the relevant stakeholders. Due to the fact that the information security committee is chaired by a CIO or a top management representative, the information security efforts also demonstrate that the idea originated from the top management.
			Democratic *(both ways)*	Both top-down and bottom-up efforts are being implemented to improve information security. It will be top-down if the government's Chief Secretary (KSN) issues detailed orders to all government agencies through a joint meeting. These instructions will be communicated to the appropriate department or team, in this case, the information security team. The team is accountable for carrying out the obtained instructions.

No	Theme	Sub-Theme		Description
				Typically, the bottom-up strategy involves proposals from the information security team itself. In the event of an information security issue, the information security team will devise a remedy and bring it to the attention of top management for approval. It is essential to guarantee that each programme is implemented efficiently. Through meetings, top management supervises the implementation process.
		Platform to discuss information security	Top management meeting	Information security is not often covered in executive meetings. If an information security issue is highlighted or a decision must be made regarding information security, the CIO will bring the matter up in the management meeting.
			Steering Committee for ICT and Security (JPICT)	Top-level management meetings include a broad range of topics pertaining to an organisation's whole business, including information security. Due to the extensive agenda, top management delegates authority to an ICT steering committee or JPICT. The purpose of establishing this committee is to ensure that security-related issues are thoroughly addressed. JPICT is the highest platform for determining the direction of information security and ICT-related issues. The committee is chaired by the Secretary-General (KSU) or the Chief Information Officer (CIO), who is also a member of the top management. JPICT members comprise each agency's undersecretaries, ICT managers, and chief information officers (if the organisation has multiple agencies). Through this platform, endorsement of information security policy occurs.
			Committee for ISMS	The CIO chairs the ISMS committee. This committee thoroughly discusses information security actions. Through this committee, the CIO will supervise

No	Theme	Sub-Theme		Description
				the audit activities of the information security team and other relevant parties within the scope of the ISMS audit. Any matters discussed herein will be brought to JPICT for endorsement if necessary.
		Top management practices in governing information security	Compliance with the public sector's information security direction	Top management ensures that any information security activities are aligned with the Public Sector ICT Strategic Plan and the customer charters of each organisation. The information security team translates top management's information security direction through information security projects and activities.
			Communication of information security awareness and initiative	Top management is critical in instilling in government employees the necessity of protecting information security. Top management promotes information security awareness through platforms, including meetings, monthly gatherings, workshops, briefings, and opening ceremonies, which the CIO coordinates. The details of the information security policy are included in the top management's speech to ensure that public officials do not leak information. Top management also works with and supports the information security team on all projects and operations. The commitment is either physical or moral support. Top management will ensure that all stakeholders understand and support the information security activities that are executed. Every initiative carried out within the organisation must be informed and promoted by management. Top management will consult with the information security team if an issue arises.
			Enforcement against information	The issue of information leakage among public officials is of great concern to top management. If classified information or documents are leaked, the subject will be discussed and investigated to decide what action should be

No	Theme	Sub-Theme		Description
			security misconduct	taken against the employee. Top management will occasionally do spot checks and surprise visits to all departments. Among the actions taken were verbal and written warnings, which might lead to more serious consequences like reporting to the police or being dismissed.
		Information security budget	Approved information security budget	One method of allocating a budget is through each department of the organisation. The budget for the information security project is allocated to the IT Division and distributed based on the project's priority within the unit.
			Case-based budget approval	Financial constraints have traditionally plagued public sector organisations. Each department responsible for implementing the ICT project must compete for a budget. Through JPICT, the entire ICT project, including information security, will be evaluated and ranked based on the importance of the project. Therefore, the strength of the information security team's explanation is essential for ensuring that each security project has an adequate budget.
		Employee competency development in information security	Training for information security employees	Information security training is not mandatory for all employees. Priority is given to personnel who handle systems and information security directly. As employees do not remain in the same position for extended periods, training is always provided to new employees tasked with taking over the position.
			Information security awareness to all employees	The security team instils information security awareness in all employees through training and briefing sessions. Briefings are sometimes held in partnership with other agencies responsible for physical documents, and officials from the Chief Government Security Office (CGSO) are invited to provide security-related information encompassing all elements - physical and online.

No	Theme	Sub-Theme		Description
		Monitoring of information security implementation	Presentation by the information security team in meeting/audit meeting	Top management frequently evaluates the execution of information security through reports from the information security team. These reports will be presented during meetings to solicit top management feedback.
			Establishment of committee	Establishing an information security committee is another method of monitoring information security implementation. They would closely oversee each information security initiative through such a committee. They also allow the information security team to propose thoughts and proposals on information security, which is taken into account.
			Information security reports or meeting minutes submitted to top management	The information security team's reporting on information security is given in simple language, with basic analogies and words, and is not overly technical so that top management understands what is being reported. The information security team's reports or meeting minutes are critical for monitoring and assisting top management in decision-making.
2	Factors Influencing Top Management Engagement in	External factor	Regulatory forces	This factor involves external regulation pressure influencing top management engagement in information security. External regulations include directives from the Cabinet, instructions, circulars, and regulations from the Chief Government Security Office (CGSO), MAMPU and other higher authoritative bodies.

No	Theme	Sub-Theme		Description
	Information Security *(Address Research Question 2)*		Imitating good practice	Top management attempts to emulate other ministries or agencies, especially MAMPU, to make their organisations' information security initiatives better or equivalent to those of other organisations. Their involvement in information security is influenced by their inclination to compete with peer organisations.
			Changes in security risk exposure	In the event of persistent challenges outside their organisation, top management is encouraged to engage in information security. For example, political upheaval in the country, the government's decision to hike petrol prices, and the implementation of the GST system, to name a few – have resulted in public displeasure and attacks on government agency websites. In addition, it is vulnerable to domestic and international challenges, requiring top management to be more aware and cautious so that their classified information is not compromised.
			Audit compliance	Top management engagements in projects and information security activities can be seen in external audits involving information security in their organisations. Examples of auditing are ISMS and the Malaysian Government Performance Index (myGPI) (previously known as System Star Rating (SSR)). In myGPI, if there is a lack in any component, it will affect the organisation's rating. Also, top management is very concerned with accreditation from external agencies such as Standard of Industrial and Research Malaysia (SIRIM), CyberSecurity Malaysia (CSM) and other international awards because such validation makes them proud of their organisational achievements. In addition, obtaining validation from external bodies will increase the organisation's trustworthiness among stakeholders.

No	Theme	Sub-Theme		Description
		Organisational factor	Reputation	Top management seeks acknowledgement in order to improve the organisation's reputation and image. Organisations gain recognition in many ways, for example, by participating in competitions or receiving certificates or letters of appreciation from renowned international and local bodies. They "compete" with other ministries and agencies to demonstrate that their organisation is the best regarding information asset protection. The accomplishments of central agencies such as Case 1 and 3 are critical in boosting their image as a reference point for other ministries and agencies.
			Information security risk awareness	Due to technological advances and the widespread adoption of social media, sensitive information can easily be compromised and shared with individuals who are not authorised to receive it. When there are events involving sensitive details being compromised intentionally or accidentally, especially within the organisation, top management engagement in information security is started to be visible. In the absence of security issues or occurrences, however, they adopt a passive stance. Top management will only become involved in the event of a problem related to the organisation's information security.
			Information security committee structure	Top management demonstrates their commitment to information security by serving on information security committees in their organisations. Their participation is achieved through the formation of committees such as JPICT. One of the objectives of forming such a committee is to increase top management engagement in information security. It is common practice for top management to be assigned roles on a security committee; thus, they are committed to their duty.

No	Theme	Sub-Theme		Description
			Culture	This factor relates to an organisation's culture. Firstly, it is the competitive culture in which information security initiatives are made to be the top management's KPI. Consequently, they participate in information security to ensure that their organisations meet the KPI. Secondly, the culture in which those (top management) voice their thoughts vocally will be given additional responsibilities. Those who do not wish to do additional tasks are likely to remain reticent and less engaged in any security program. As a result, top management is more reluctant to express their opinions, conceal the fact that they are knowledgeable in the area of security, or engage in information security activities because they do not wish to be burdened with related responsibilities in the future. Lastly, in security-related committees, information security is a fixed agenda in the meeting. When the topic is persistently mentioned in discussions, it may increase the top management's awareness of security issues and encourage their engagement in information security activities.
		Personal factor	Informal education	Participation of top management in information security initiatives may be influenced by their interest, awareness, and knowledge of the domain. This element takes into account scenarios in which top management is engaged in information security, as demonstrated by his experience managing numerous organisations, communicating with other peers professional in other organisations, and managing government directives on information security or other relevant platforms. Next, they have a reasonable understanding of the significance of information security, leading to their

No	Theme	Sub-Theme		Description
				competency. Finally, he has gained an understanding of information security through self-exploration and reading.
			On-the-job exposure	The job experience or work assignment of top management in the organisation influences their engagement in information security. For example, public officials constantly shift duties, moving from one ministry/agency to another. The work experiences they gathered while serving in past organisations will shape their role in information security at the current ministry/agency. The same can be said about work assignments. While top management may not have a background in information security education, they must be aware of and involved in information security in order to achieve their job responsibilities.
			Formal education	Education in information security from academic institutions may result in diverse interpretations and perspectives on information security, which influence the involvement of top management in information security. Other ways to acquire information security expertise include professional training, seminars, and so on.
3	Information Security Governance Issues	Top management constraint	Limited bandwidth due to hectic schedule and various meeting agenda	The schedule of top management is always demanding. The majority of time is spent coordinating meetings and activities within and outside of the organisation. As a result, the majority of information security issues are assigned to the information security team to manage.

No	Theme	Sub-Theme		Description
	(Address Research Question 3)		Inadequate knowledge and experience in information security	Information security management challenges include the understanding of information security at the top management level. As a result of delegating the responsibility to the information security team, government management is less interested in information security issues. They rely on the information security team to provide advice and update them on information security issues. Their knowledge of information security influences their governance practises in information security.
			Reactive in handling information security issues	Information security is discussed and given particular attention whenever issues and incidents occur within or outside the organisation.
			Information security is not an integral part of the organisation's business	Initiatives pertaining to information security receive the least amount of attention from the top management because of their perspective that information security is more of a support function for the organisation rather than an essential component of its operations. As a result of the lack of quantitative information that top management needs to have in order to optimise security investments, security projects are given less importance (monitoring, budget, etc.) than projects in other disciplines. IT Division needs to make strong justification so that projects under information security can be visible and thus prioritised by the top management.
			Generation gap of top management	The majority of top management is from the baby boomer generation, who has had less exposure to technology. As a result, when information security issues are brought up, they find it difficult to grasp the concept and give it

No	Theme	Sub-Theme		Description
				some thought. As a result, they rely on the information security team or other middle management to aid them in decision-making.
		Resource constraint	Insufficient budget allocation	Implementing information security initiatives involving upgrading existing resources has been an issue due to financial constraints. Due to these constraints, organisations must use all available resources to ensure that their information assets' security is maintained despite not investing in the latest security technologies.
			Insufficient human capital	The information security team is in charge of implementing information security strategies throughout the organisation. However, because of the limited size of the team, employees with no background in ICT education must collaborate to satisfy information security and ICT demands, despite the fact that this is not their area of competence.
		Challenges in employee acceptance of information security	Difficult to control staff	Top management must ensure that a large number of employees or agencies follow information security regulations at all times. Support personnel are among those who have an excess of classified papers and information. It is also difficult to control organisational information released on social media. These are the main managerial challenges in protecting the security of their organisation's information assets.
			Employee lack of information security awareness	There is a problem where employees do not fully comprehend information security implementation-related topics. The idea that information security is irrelevant to them or that compliance with the information security policy hinders their daily activities must be revised. It is a challenge for top management and the information security team to guarantee that the entire

No	Theme	Sub-Theme		Description
				organisation comprehends all initiatives. Everyone contributes, directly or indirectly, to the success of the organisation's information security activities.
		Organisation's culture	Focus only on passing audit compliance	The established information security initiatives are more concerned with achieving certification audits than protecting the information assets. The focus is more on personnel and matters within the scope of the audit.
			The misconception of information security and ownership	There is a misconception that information security is usually associated with the IT Division since they only refer to technical solutions for information security. However, preserving information assets requires top management and all employees' responsibilities and making it a culture. The employees and top management also preconceived notions of the information security team's function. Information security initiatives are complex to realize when management does not appreciate the matter and its relevance, which lead to a bottom-up approach.
			Difficult to change job routines	It is not easy to alter the habits of individuals inside an organisation in order for them to comply with information security policy. They anticipate that the workload will increase in order to ensure compliance with the regulation, resulting in a slow and laborious process. Since there is a view that information security is generally the duty of the IT Division and the information security team, obtaining collaboration from other departments to implement information security initiatives throughout the organisation is difficult. It becomes a challenge for top management to instil a culture of information security so that employees no longer perceive their work as burdensome.

As stated in Chapter 2, the initial research model, which adapted the Multiple Perspective Concept and Neo-Institutional Theory in Figure 2.11, serves as a guide in setting up the structure for interview questions and categorizing research findings into themes and sub-themes, as depicted in Table 4.1.

4.3 RESEARCH FINDINGS

The previous section covers the data analysis, which comprises the generation of themes and sub-themes (Table 4.1) and descriptions (Table 4.2). Moving forward, this section presents the research findings based on the analysis. These findings are arranged according to the research questions in sequence, and in each of the research questions (RQ1 until RQ3), there are three (3) sections (themes) to be elaborated on; starting from Theme 1: Information Security Governance Approach, followed by Theme 2: Factors influencing Top Management Engagement in Information Security, and lastly, Theme 3: Information Security Governance Issues.

4.3.1 Theme 1: Information Security Governance Approach

Theme 1 refers to how top management in public sector organisations administer and lead information security initiatives. This categorization is developed to understand how top management in each organisation is involved in information security governance. As this research explores the factors that influence the engagement of top management in information security governance, the researcher first needs to identify the leadership style implemented in the organisation. Then, on which platform is often the matters related to information security are discussed, and the current practice by the top management in driving information security initiatives within their respective organisations. These include allocating resources for information security programs conducted, competencies programs for the employees, and how the top management monitors information security activities implemented, including actions on the non-compliance of information security policies carried out by employees within their organisation. After comprehending and gaining a deeper grasp of the top management's

approach to managing information security inside their organisation, the factors that impact their engagement in information security may be derived to fulfil research question 2. The following section discusses the findings for each sub-theme under Theme 1. Table 4.3 summarizes the analysis result for the information security governance approach (Theme 1) based on the case and by designation in Table 4.4.

Table 4.3: Theme 1 – Information Security Governance Approach based on case

Sub-Theme		**Case 1**	**Case 2**	**Case 3**	**Case 4**	**Total All Cases**
Top management leadership style in governing information security	▪ Laissez-Faire (bottom-up)	1/8	3/8	2/4	0/7	6/27
	Percentage (%)	12.5	37.5	50.0	0.0	22.2
	▪ Authoritarian (top-down)	1/8	3/8	2/4	2/7	8/27
	Percentage (%)	12.5	37.5	50.0	28.6	29.6
	▪ Democratic (both ways)	2/8	1/8	1/4	2/7	6/27
	Percentage (%)	25.0	12.5	25.0	28.6	22.2
Platform to discuss information security	▪ Top management meeting	1/8	0/8	1/4	3/7	5/27
	Percentage (%)	12.5	0.0	25.0	42.9	18.5
	▪ Steering Committee for ICT and Security (JPICT)	3/8	6/8	3/4	4/7	16/27
	Percentage (%)	37.5	75.0	75.0	57.1	59.3
	▪ Committee for ISMS	0/8	6/8	1/4	3/7	10/27
	Percentage (%)	0.0	75.0	25.0	42.9	37.0
Top management practices in	▪ Compliance with the public sector's	6/8	3/8	2/4	3/7	14/27

Sub-Theme		Case 1	Case 2	Case 3	Case 4	Total All Cases
governing information security	information security direction					
	Percentage (%)	75.0	37.5	50.0	42.9	51.9
	▪ Communication of information security awareness and initiative	1/8	5/8	4/4	7/7	17/27
	Percentage (%)	12.5	62.5	100.0	100.0	63.0
	▪ Enforcement against information security misconduct	3/8	1/8	1/4	1/7	6/27
	Percentage (%)	37.5	12.5	25.0	14.3	22.2
Information security budget	▪ Approved information security budget	3/8	4/8	0/4	3/7	10/27
	Percentage (%)	37.5	50.0	0.0	42.9	37.0
	▪ Case-based budget approval	1/8	2/8	1/4	3/7	7/27
	Percentage (%)	12.5	25.0	25.0	42.9	25.9
Employee competency development in information security	▪ Training for information security employees	6/8	1/8	1/4	2/7	10/27
	Percentage (%)	75.0	12.5	25.0	28.6	37.0
	▪ Information security awareness to all employees	8/8	7/8	4/4	7/7	26/27
	Percentage (%)	100.0	87.5	100.0	100.0	96.3

Sub-Theme		Case 1	Case 2	Case 3	Case 4	Total All Cases
Monitoring of information security implementation	▪ Presentation by the information security team in meeting/audit meeting	2/8	8/8	3/4	5/7	18/27
	Percentage (%)	25.0	100.0	75.0	71.4	66.7
	▪ Establishment of committee	0/8	0/8	1/4	2/7	3/27
	Percentage (%)	0.0	0.0	25.0	28.6	11.1
	▪ Information security reports or meeting minutes submitted to top management	1/8	8/8	3/4	4/7	16/27
	Percentage (%)	12.5	100.0	75.0	57.1	59.3

Table 4.4: Theme 1 – Information Security Governance Approach based on designation

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
Top management leadership style in governing information security	▪ Laissez-Faire (bottom-up)	1/4	4/11	1/12	6/27
	Percentage (%)	*25.0*	*36.4*	*8.3*	*22.2*
	▪ Authoritarian (top-down)	2/4	5/11	1/12	8/27
	Percentage (%)	*50.0*	*45.5*	*8.3*	*29.6*

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
	▪ Democratic (both ways)	2/4	4/11	0/12	6/27
	Percentage (%)	*50.0*	*36.4*	*0.0*	*22.2*
Platform to discuss information security	▪ Top management meeting	1/4	1/11	3/12	5/27
	Percentage (%)	*25.0*	*9.1*	*25.0*	*18.5*
	▪ Steering Committee for ICT and Security (JPICT)	3/4	8/11	5/12	16/27
	Percentage (%)	*75.0*	*72.7*	*41.7*	*59.3*
	▪ Committee for ISMS	1/4	7/11	2/12	10/27
	Percentage (%)	*25.0*	*63.6*	*16.7*	*37.0*
Top management practices in governing information security	▪ Compliance with the public sector's information security direction	3/4	6/11	5/12	14/27
	Percentage (%)	*75.0*	*54.5*	*41.7*	*51.9*
	▪ Communication of information security awareness and initiative	4/4	9/11	4/12	17/27
	Percentage (%)	*100.0*	*81.8*	*33.3*	*63.0*

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
	▪ Enforcement against information security misconduct	1/4	2/11	3/12	6/27
	Percentage (%)	*25.0*	*18.2*	*25.0*	*22.2*
Information security budget	▪ Approved information security budget	3/4	6/11	1/12	10/27
	Percentage (%)	*75.0*	*54.5*	*8.3*	*37.0*
	▪ Case-based budget approval	0/4	6/11	1/12	7/27
	Percentage (%)	*0.0*	*54.5*	*8.3*	*25.9*
Employee competency development in information security	▪ Training for information security employees	0/4	1/11	9/12	10/27
	Percentage (%)	*0.0*	*0.1*	*75.0*	*37.0*
	▪ Information security awareness to all employees	3/4	11/11	12/12	26/27
	Percentage (%)	*75.0*	*100.0*	*100.0*	*96.3*
Monitoring of information security implementation	▪ Presentation by the information security team in meeting/audit meeting	3/4	11/11	4/12	18/27

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
	Percentage (%)	*75.0*	*100.0*	*33.3*	*66.7*
	▪ Establishment of committee	1/4	0/11	2/12	3/27
	Percentage (%)	*25.0*	*0.0*	*16.7*	*11.1*
	▪ Information security reports or meeting minutes submitted to top management	3/4	10/11	3/12	16/27
	Percentage (%)	*75.0*	*90.9*	*25.0*	*59.3*

4.3.1.1 Sub-Theme 1: Top Management Leadership Style in Governing Information Security

When it comes to leading, inspiring, guiding, and managing groups of employees in relation to information security initiatives within an organisation, a leadership style refers to the characteristic behaviours of top management. The researcher adopted the three (3) categorizations of leadership style from one of the oldest and probably the most common mentioned today by Lewin et al. (1939), a group of behavioural psychologists. Those scholars elaborated the leadership style categorization in their leadership style framework, as depicted in Table 4.5.

Table 4.5: Three (3) types of leadership style

No	Authoritarian	Democratic	*Laissez-faire*
1	All determination of policy by the leader	All policies are a matter of group discussion and decision, encouraged and assisted by the leader	Complete freedom for group or individual decisions, without any leader participation
2	Techniques and activity steps were dictated by the authority, one at a time, so that future steps were always uncertain to a large degree	Activity perspective gained during the first discussion period. General steps to group goal sketched, and where technical advice was needed, the leader suggested two or three alternative procedures from which choice could be made	Various materials were supplied by the leader, who made it clear that he would supply information when asked. He took no other part in work discussions
3	The leader usually dictated the particular work task and work companions of each member	The members were free to work with whomever they chose, and the division of tasks was left up to the group	Complete nonparticipation by the leader
4	The dominator was "personal" in his praise and criticism of the work of each member but remained aloof from active group participation except when demonstrating. He	The leader was "objective" or "fact-minded" in his praise and criticism and tried to be a regular group member in spirit without doing too much of the work	Very infrequent comments on member activities. Unless questioned, and no attempt to participate or interfere with the course of events

No	Authoritarian	Democratic	*Laissez-faire*
	was friendly or impersonal rather than openly hostile.		

4.3.1.1.1 Laissez-Faire, Authoritarian, and Democratic

In Case 1, there are different views on the leadership style that top management practices in their organisation related to information security administration. The CIO mentioned that, in general, the leadership style in the organisation is both ways, but if there are any instructions or mandates from the cabinet or ministers, it will turn into top-down:

> It can be from top-down or bottom-up. Usually, instructions that are applied to all agencies will be informed via a meeting with the Chief Secretary to The Government (KSN). Then (after the meeting), the Director-General will inform of things that need to be done. Sometimes the IT Division will be the one who makes recommendations, including actions that need to be implemented. The recommendations could be anything from avoiding the events (information security incidents) or making the agency well prepared to handle the event if it were to happen again in the future (1:16_Line 48_A1TM1)

The statement was agreed upon by one of the information security personnel. However, there was a view from one of the heads of the IT Division said that, based on his experience working with top management, especially concerning information security, the style is more bottom-up, where the information security initiatives usually come from the IT Division itself and bring up for approval (if necessary) as in the following quotation:

> Based on my experience working with top management, this (information security initiative) comes from the IT Department. Other units are not involved. But in a specific program like drafting DKICT (information security policy) for the organisation, we will invite representatives from all departments. Usually, only one or two representatives are invited. And they are not top management. After the process, it will be brought up to the top management for approval. For approval, I am not sure if the information security policy will be presented or not during the top management meeting. I am not sure. To date, and as per my knowledge, it is not presented. The meeting will just be informed that an information

> security policy has been drafted. I think CIO will review it before the meeting (8:11_Line 171_A1NIS6)

For Case 2, only the CIO stated that the way they manage the information security-related matters is both ways:

> We implement two ways. For example, the IT division will prepare the planning and the details. Then need to get the approval of top management. That is the source of power (top management instructions). Implementation will start once it is approved. We consider it as two-way (9:5_Line 43_A2TM1)

Six (6) out of seven (7) personnel thought that the top management practices either bottom-up or top-down:

> ICTSO's role entirely to assess any issues related to security (information) and inform top management of actions to be taken. In my opinion, this (ICTSO role) will continue as long as the CIO is not from technology, communication, or, to be more specific, cybersecurity background. Maybe one day. There is a plan for the CIO to have a technology background. (When this happens) Probably things will be a little bit different—just my opinion. As of now, middle level to this (up). Bottom to up, yes. Most of the time (10:19_Line 105_A2IS1)

On the other hand, top management from Case 3 has a different opinion from other top management in Case 1 and Case 2. He argues that top management in his organisation adopts a bottom-up approach:

> From then until now, the Security Section or the Security Division will initiate matters involving information security, and then only brought to top management for approval (20:12_Line 115_A3TM1)

One (1) out of two (2) personnel from the information security unit agreed with the top management's statement. All information security personnel also added that the leadership style would be top-down if there were instructions from the central agency:

> In my opinion, that (top-down) is not suitable because we at this level inform top management. The awareness happens when the middle (executives) level informs everybody, not the other way round (top-down) (17:5_Line 38_A3IS1)

The CIO for Case 4 mentioned that, even if the information security implementation has been handed over to the IT Division, the top management is still responsible for deciding the overall course of information security in the organisation:

> Information security direction is still determined at the top management level (21:29_Line 234_A4TM1)

This claim was supported by only one (1) information security personnel and added that the leadership style is top-down if there is a mandate or instructions from an authoritative body or central agency like MAMPU:

> When our top management received information (notification, instructions) from agencies like MAMPU, which requires us to implement specific actions like security reinforcement, they will inform us in our department meetings (22:7_Line 55_A4IS1)

However, among all four (4) information security personnel, two (2) argued that their top management style governing information security is both ways.

Based on the findings of all the case studies, it can be seen that there are mixed opinions among all participants. Two (2) out of four (4) CIOs and top management said that the way they administer information security is both ways, and the rest says bottom-up or top-down. Information security personnel and non-information security personnel also have different views in determining leadership style by top management. However, according to the observations and overall inputs of the interview sessions with all participants, in general, the leadership style practised in all four (4) organisations is a combination between Democratic (both ways) and Laissez-faire (bottom-up) based on categorization by Lewin et al. (1939). Most of the time, the top management gives the IT Division total freedom to determine the implementation of information security within their organisation (Laissez-faire). However, everything needs to be reported to top management:

> Top Management plays a role in every information security initiative as they are the Chairman of the ICT Steering Committee, Information Security Audit and more. Most information security-related matters will be notified on the platform for their advice. We need to report because we need to adhere to the hierarchy in the organisation (17:9_Line 49_A3IS1)

Since three (3) out of four (4) CIOs interviewed do not have a background in information security education or at least have formal education in the field of information technology, dependency on the IT Division in providing directions and implementing information security activities is very high (Democratic):

> First of all, we (top management) will see the importance of implementing an information security initiative, whether important or not, and what the implication is. IT division should justify. Then, we will look at our capabilities. If necessary, we will do it. Of course, it all

> depends on the justification of the IT Division. So we rely heavily on the input provided by IT Division (1:28_Line 101_A1TM1)

Top management engagement in implementing information security is limited except through some matters initiated by the IT Division. The engagement involves providing comment and endorsement on the information security policy developed by the IT Division and giving consent to the information security activities to implement within the organisation (Laissez-faire) as informed by one of the following respondents:

> Usually, we will formulate a security policy at the Division level. Then we will present at the top management level to get consent. Every comment and improvement will be taken into account, and we will refine it again. We will include their views to strengthen our security policies (24:1_Line 29_A4IS3)

4.3.1.2 Sub-Theme 2: Platform to Discuss Information Security

In general, three (3) main platforms are employed in all case studies that address all aspects of information security i.e., Top Management Meeting, Steering Committee for ICT and Security (JPICT), and Committee for ISMS. Because all case studies involve ministries and government departments, the platform used to discuss information security issues is similar.

4.3.1.2.1 Top Management Meeting

Information security is not discussed regularly in top management meetings. If an information security issue is raised or the need for a decision on information security to be made, the CIO will bring the matter to the management meeting as mentioned by the CIO of Case 4:

> Overall, any reporting will be made by the division (IT Division – the information security team). The division will execute the process, and I will monitor whether the process is done thoroughly or otherwise. So I will bring the results and report them to the management meeting. We will present each time an activity is carried out, and we will present it in a management meeting. So top management will get to monitor closely (21:27_Line 38_A4TM1)

All case studies mentioned that in the top management meeting, there is no fixed agenda to discuss information security matters except when an issue arises, as told by the following non-information security personnel from Case 1:

> For information security matters that need to be raised or require a decision of the top management, the matter will be brought to the MPT (top management meeting). Like the CIO's meeting (JPICT) – discuss in detail first, and in order to obtain a mandate from the top management, the matter will be brought into the management meeting (5:22_Line 118_A1NIS3)

This statement is also supported by another non-information security personnel from Case 3:

> It has no fixed agenda (regarding information security), just a periodic agenda in the management meetings. All top management and department directors are the members in this management meeting (19:12_Line 98_AS3NIS1)

An information security personnel from Case 4 mentioned that the top management meeting discusses general matters regarding the organisation's management and core business issues. The members of this management meeting are the same members attending the JPICT meeting, which consists of representatives from all departments in the organisation:

> The members are the same; the contents of these meetings are different. In the management meeting, the discussion is on general matters related to SPA management. This meeting will involve all departments. But in JPICT, we will explain our (IT and information security) actions/activities in supporting the organisation. JPICT can be considered a catalyst to what we want to plan, based on the department's annual requirements (24:7_Line 61_A4IS3)

4.3.1.2.2 Steering Committee for ICT and Security

Top management meetings discuss various agendas covering an organisation's core business management. Since there is much agenda to discuss, matters involving information technology, including information security, are delegated to another committee called Steering Committee for ICT and Security (JPICT), as claimed by the CIO from Case 1:

> The top management has many things they need to oversee. So I think it is appropriate for CIO to filter issues which need further discussion with

> the top management. If not, the top bosses will have so much to do (1:43_Line 159_A1TM1)

This is supported by one of the personnel from Case 1:

> MPT (top management meeting) always lasts for 3 hours, and tons of issues related to the organisation are discussed. Even though the meeting is convened once every two weeks, there is still not enough time to discuss specific matters like ICT. Because of this, they delegate the power to JPICT, chaired by the CIO, to discuss in detail (about ICT) (5:21_Line 112_A1NIS3)

This committee's establishment is to ensure that issues related to security are addressed in detail and comprehensively. JPICT is the highest platform that determines the direction of information security and all matters in ICT:

> Steering Committee for ICT (JPICT) is the highest committee in the department. Discussion on matters related to ICT security controls has become a fixed agenda in the JPICT meeting. The issue (ICT security controls) is always discussed in that meeting (15:1_Line 44_A2NIS2)

The committee is usually chaired by the CIO (Case 1, 3 and 4) or the Secretary-General (KSU) (Case 2), who is also a member of the top management. JPICT members are among each department's head, including ICT managers and CIOs of each agency (if the organisation has multiple agencies under it):

> JPICT has a fixed agenda. In the fixed agenda, we will present security issues. KSU chairs it (11:24_Line 177_A2IS2)

Top management, through the CIO, provides input and feedback during the information security policy development. This pertains to the draft of the information security policy prepared by the IT Division, particularly the information security team. After completing the enhancements, the CIO is responsible for approving the information security policy before it can be implemented across the organisation. Through JPICT, information security policies are endorsed:

> We integrate input from the top management (for information security policy). Then we present them in JPICT for endorsement" (2:5_Line 29_A1IS1)

4.3.1.2.3 Committee for Information Security Management System

The standards for developing, executing, monitoring, evaluating, maintaining, and upgrading an organisation's information security management system are established in ISO/IEC 27001, the international standard for Information Security Management System (ISMS). A management system compliant with this standard should secure the organisation's information's confidentiality, integrity, and availability to demonstrate that it meets the standard's requirements (SIRIM QAS International, n.d.). Therefore, organisations subscribe to the audit program and apply the standard to take advantage of the best information security practices it provides. In contrast, others want to become certified in order to demonstrate to customers and clients that their recommendations have been followed (International Organisation for Standardization, n.d.-a).

Following the Cabinet directive for ISMS certification in every ministry and agency, top management agrees to implement the respective organisations' certification. Several budgets are provided for this purpose. The ISMS is established to monitor and carry out this audit activity led by the information security team in IT Division. On behalf of top management, the CIO demonstrated cooperation in the ISMS audit by officiating the audit workshop and meeting. In obtaining/maintaining ISMS certification, the CIO engages in the management review phase and the endorsement and approval of documents such as information security policy. The CIO may also consider expanding the scope of the audit once the certification has been obtained.

From Case 1 to Case 4, the CIO chairs the ISMS committee. Through this committee, information security audit activities are discussed in detail. The CIO's involvement in information security is as a chair of ISMS management committee meetings. The CIO will monitor the audit work carried out by the information security team and other parties within the ISMS audit scope as told by the CIO from Case 2:

> We will look at the meeting. It is not just a regular presentation; all the weaknesses will be elaborated on – what audit findings were received and what suggestions for improvement. So, from there, our role as top management is for endorsement. Indirectly, we know what the problem is. That is our style (9:15_Line 113_A2TM1)

If necessary, any matters discussed in the ISMS meeting will be brought to JPICT for endorsement, for example, the revised version of the information security policy:

> The ISMS Committee discusses explicitly the implementation of ICT security involving the scope of our organisation. CIO chairs the committee. The committee consists of ICTSO and all implementers involved in the scope. The discussion will touch on our implementation, monitoring, whether all policies have been decided, whether there is compliance by all, review, etc. So, all those things will be discussed in the committee. If there are issues that cannot be resolved at this stage, we will bring them to the Steering Committee (JPICT) (15:43_Line 44_A2NIS2)

4.3.1.3 Sub-Theme 3: Top Management Practices in Governing Information Security

This sub-theme describes how top management, specifically the CIO, leads and manages all information security initiatives in their organisation. The pattern for each case study is nearly identical since the CIO (except in Case 2, which the Director-General (KSU) chairs) heads the IT steering committee and information security audit. Furthermore, since IT administration and information security have been delegated to JPICT, the CIO plays an essential role in ensuring that the information security direction in their organisation is consistent with the public sector's security direction. Furthermore, top management is responsible for issuing warnings, raising awareness among all employees about the necessity of preserving information security, and taking action against employees who have contributed to the leakage of organisational and government-level information.

4.3.1.3.1 Compliance with the Public Sector's Information Security Direction

Top management ensures that any information security initiatives align with the Public Sector ICT Strategic Plan and each organisation's customer charters. The CIO from Case 1 and 4 and top management of Case 3 shared a similar view regarding the alignment of information security initiatives within their organisation so that it would

not deviate from the government's aspirations. The top management from Case 3 stated that:

> About that, the alignment starts at the early stage. One of the Information Security Strategic Plan (ISP) components of 2016-2020 is the Public Sector Information Security Framework (RAKKSA). So, all our efforts are based on and within the framework. The same goes for getting approval for all ICT projects related to information security; it must have the source of authority (punca kuasa). So, from the beginning until you present it for approval, it must be aligned to the framework. During the JPICT, we ensure all presented projects are aligned to the RAKKSA and ISP. If not, they need to present it again (20:14_Line 136_A3TM1)

The CIO of Case 1 also supports this as follows:

> Before they draft it (information security policy), we will provide them with some input. Of course, the IT Division will inform us about the requirements in DKICT (ICT security policy), why it is needed and other related issues as long as it is in line with the head of the department's vision and aligned with the public service's overall need (1:13_Line 41_AITM1)

The CIO of Case 4 added that the information security activities in her organisation should be in line with the client charter:

> In that aspect, we have our customer charter. Confidentiality, integrity and others have long been part of the charter's objective. So, as I mentioned before, we will oversee all activities and processes, except if there are any issues (21:10_82_A4TM1)

Top management's information security direction is translated through information security projects and activities carried out by the information security team, as mentioned by one of the information security personnel from Case 4:

> It (the direction of the information security) must come from the top management. Anything must come from the top management before those at the lower level execute the tasks based on that direction (23:7_103_A4IS2)

4.3.1.3.2 Communication of Information Security Awareness and Initiative

The role of top management in communicating to government personnel the significance of ensuring information security is vital. Top management promotes information security awareness represented by the CIO through meetings, monthly gatherings, workshops, briefings, and opening ceremonies. The contents of the

information security policy are incorporated in the speech of the top management to guarantee that employees do not contribute to information leakage. The CIO from Case 1 quoted that:

> From time to time, we will remind them of the dangers. Maybe during meetings or our monthly assembly, we will remind them again of the importance. We will highlight cases reported in the newspaper related to information leakage and the problems it caused. This means we provide awareness to them (1:20_Line 67_AITM1)

The statement from the CIO was supported by one (1) of the non-information security personnel as the following:

> In meetings, it is said the top management always issues reminders. Particularly with the increased number of cases that went viral, top management is cautious about classified information issues; the implication of these issues. There is always a constant reminder, even in the Cabinet and post-cabinet meetings. It is a frequent topic discussed (4:3_Line 194_A1NIS2)

One (1) of the information security personnel from Case 4 also mentioned that their top management fully commits to information security activities in their organisation:

> In terms of commitment, top management, including the CIO, do give their total commitment to the implementation of information security. First, whenever there are activities that involve security components, they will participate and show their support to us. Then, through divisions meeting platform, they emphasise the importance of protecting data confidentiality and related issues (24:32_Line 316_A4IS3)

As for Case 2, there are times when the information security team will take advantage of a meeting or particular event to deliver an awareness campaign to the members of the meeting or all attendees. From that point on, the top management will emphasize and urge everyone on the need to adhere to the awareness campaign by the information team:

> So in some meetings or events, we will brief everyone about matters related to information security. He (the CIO) will be aware of it and ask the meeting members to comply. So it becomes awareness briefings (13:7_Line 33_A2IS4)

Top management will ensure that all employees comprehend and support established information security activities. The commitment is mainly one of moral support. Top management will personally discuss with the information security team should any issue arises, as told by information security personnel from Case 3:

> Top management like the CIO, Deputy Director-General, and the Director-General will get involved, especially in problematic projects. A security-related project once had issues, so the team, including top management, stayed back that night. They sit together in the meeting room. For me, that shows top management's commitment. They instructed us to stay back, and they did the same. That is in our organisation (18:15_Line 133_A3IS2)

4.3.1.3.3 Enforcement Against Information Security Misconduct

Top management is very concerned about the issue of information leakage among civil servants. In the event of classified information or document leakage, the matter will be brought to the meeting for discussion and investigation to determine what action should be taken against the employee. Top management will sometimes make spot checks and surprise visits to each department. Among the actions taken were to give verbal and written warnings, leading to more severe punishments such as reporting to the police or being fired, as mentioned by the CIO of Case 1:

> For these people, we will reprimand them. If it is proven they do not follow it and compromise security, we will take action. We will first issue a warning to them. If they refuse to comply, we will take more drastic action. Hopefully, with that, they will change for the better (1:22_Line 76_AITM1)

In addition, the CIO stated that she enjoys doing random workplace inspections as one of her monitoring methods:

> Sometimes, I like to do surprise checks in certain places. As a normal human being, if you sit very long in front of a computer, even if your work is not significantly related to the computer, there may be something wrong. Maybe he has no work to do, and he is watching something on the computer (1:61_Line 157_AITM1)

On the other hand, the CIO of Case 2 is planning to make a different approach where the organisation will invite external bodies, for example, the Chief Government Security Office (CGSO), to do the inspection of their organisation:

> For security, in particular, we want to introduce departmental security, and we proposed it during yesterday's meeting. I want to make sure the CGSO makes the inspectorate, do surprise visits, surprise inspections (9:7_Line 60_A2TM1)

In Case 3, top management addresses the issue of security misconduct by involving all related parties in the organisation and conducting an investigation based on evidence and in accordance with the government's rules:

> Issues related to information leakage will be handled immediately. When the problem is detected, it will involve all parties, including the top management. KP (Chief Director) himself will take action. We will follow the SOP and government circulars on record management and information confidentiality in handling such cases (19:20_Line 159_AS3NIS1)

Personnel from Case 4 stated that any security misconduct in his organisation would be reported directly to the police:

> Our management takes it very seriously about information leakage. In a few meetings in which I took part, for the top management, it was quite straightforward. If you did something wrong and are proven guilty, the case will be reported to the police. As simple as that. They will state this upfront. If you made the mistakes and were due to negligence, they will report it to the police (24:31_Line 311_A4IS3)

According to all of the statements that the participants provided, each case study focuses on information security breaches committed by their employees, and participants have indicated that disciplinary action will be taken against employees who commit such violations.

4.3.1.4 Sub-Theme 4: Information Security Budget

Public sector organisations have traditionally struggled with limited financial resources. The yearly funds each ministry or agency acquire determines how much of the available financial budget will be distributed to them. In the Malaysian public sector, two (2) different processes are used to distribute financial budgets among all of the divisions that make up their various organisations. The first way is through a financial allotment that has been made for each department. The budget is contingent on the planned projects and the results of the projects that came before them. Second, the distribution of financial resources is contingent on the project's significance. This allotment takes into account the prompt execution of the ad hoc project.

4.3.1.4.1 Approved Information Security Budget

One way of budget allocation is through each department of the organisation. The budget for the information security project is allocated to the IT Division and divided according to the project's priority within the division. According to the CIO of Case 4, a priority is usually given to making financial arrangements for carrying out tasks related to information security:

> We allocate budget, but sometimes it is sufficient, and sometimes it is not. However, in certain circumstances, for example, if we discuss licensing or anything related to ICT and security, we will prioritise. The department will prioritise them to ensure our system is always under control. They will always be the priority (21:21_Line 203_A4TM1)

Ten (10) out of 27 personnel in all case studies support the argument as quoted by one (1) of the information security personnel from Case 2 and Case 1, respectively:

> Yes, there is a budget. We always get it when we ask for a budget. The budget is assigned to the department. From there, we will manage it accordingly. There will no budget cut when it comes to security (13:36_Line 175_A2IS4)

> (Budget for security) always given the priority. So, that is one form of support we receive (2:54_Line 359_A1IS1).

4.3.1.4.2 Case-based Budget Approval

It is necessary for every department that is working on the ICT project to compete for a budget. Through JPICT, the entirety of the ICT project, including information security, will be analysed and then ranked according to the criticality of the project. Case 1's information security personnel mentioned that the top management has to evaluate and prioritise more important projects due to the tight financial budget:

> Suppose it got rejected (budget for security), not because it is unimportant. However, it is based on priority due to limited funding. As the chair of JPICT, he (the CIO) cannot entertain or focus on specific needs only. He needs to look at the overall picture. From there, he prioritised. The most important for him is what will happen if we cannot implement it (project). That is all - the impact or the outcome (2:79_Line 362_A1IS1)

For this reason, a convincing justification from the information security team is essential to guarantee an adequate budget for any security project that will be carried out:

> That also depends on how we convince him. Even if we list the project's importance, he can still cut the allocation and assign it to other projects that he deems more critical. Currently, the financial and resource budget is quite tight. He needs to consider all projects and prioritise them. Because of this, even information security needs to be convincing. For example, suppose we presented the project and requested RM3 million. In that case, he might argue that the justification is not strong enough, and he does not see the criticality of the information security project. The probability is that he will not approve the request. So it does depends on how convincing our justifications are (18:32_Line 281_A3IS2)

In the event that something unfortunate occurs, financial allocation is always seen as the first priority, as reported by information security personnel from Case 4:

> Prior to this, a department's building caught fire, which we utilise to further our argument to have a DRC (disaster recovery centre). Previously, the project manager never received the DRC budget when he requested it. Then we had to repeat each step. We presented again to the top management with the amendment, and at the same time, using the event (burned building) as evidence, the top management became more attentive and gradually approved the budget. Before this, our requests were always denied (23_17_Line 184_A4IS2)

4.3.1.5 Sub-Theme 5: Employee Competency Development in Information Security

Every public employee must have seven (7) days of training (six (6) hours per day). This includes job-specific training, speeches, seminars, and technology update sessions. One of the key performance indicators (KPI) for each ministry's Secretary-General is the completion of the 7-day training of the employees.

The training that is typically provided to employees is connected to the duties they do on the job. When it comes to information security, the personnel who are operating in the field are given priority for this training. On the other hand, there are also information security training opportunities available to other employees; however, attendance at these opportunities is voluntary, as what has been said by non-information security personnel of Case 1:

> So far, no instructions say I must go (training). There are courses and sessions which are not optional (must attend). If it is optional, I might not be joining because I am not involved directly (in information security) (7:1_Line 36_A1NIS5)

Having said that, a briefing session on the ICT Security Policy of the Ministry is a requirement that must be provided to all personnel. Each employee attending the briefing must sign a form confirming they attended and understood the ICT security policy briefing, as quoted by personnel from Case 2:

> At least once, the IT Division will make an awareness briefing on DKICT to all employees in a year. We will do a briefing and will call all the staff. After the briefing, employees will sign the DKICT form (16:8_Line 113-115_A2NIS3)

The undertaking requires the employees to implement and comply with all the information security policies. Any non-compliance with this policy will result in action and penalties being imposed as stated by personnel from Case 3:

> The DKICT binds us. All employees, including vendors, must sign a declaration letter (DKICT compliance). So we are indeed subject to that policy. If the policy is violated, action will be taken against us (18:12_Line 106_A3IS2)

Personnel from Case 2 also agreed that they must adhere to the information security policy because it is considered one of the Director-General's mandates to preserve the confidentiality of information:

> As employees here, with the existence of DKICT, we indirectly have to comply with the rules related to ICT security. When the form in the DKICT is signed, it counts as a mandate from the KSU. We must abide by this (13:15_Line 77_A2IS4)

4.3.1.5.1 Training for Information Security Employees

Employees are not required to attend training on information security if they choose to do so. The employees who are actively involved in the system and information security management are given priority, as supported by the CIO of Case 4:

> We provide training to our officers regularly, or we choose, that is, to those involved in implementing the system. It is because most of the staff involved are support groups. So we will give training to them (21:5_Line 65_A4TM1)

Because employees typically do not remain in the same position for extended periods, training is consistently provided to new workers responsible for taking over the job:

> Information security and system security always exist in the postmaster at our organisation, but security courses are more focused on ICT Officers first. I think so. ICT officers also come and go. So, to strengthen their knowledge, we will send officers who are involved directly with a system. Like HRMIS, each division has an administrative officer. That officer will be given priority. That is because he is in charge of entering all the data; he needs to ensure the data's integrity as the data can be manipulated. So the officers will be given (security training). Currently (security training) is only given to certain ones. We cannot give it as a whole; we cannot give courses simultaneously to everyone (5:5_Line 70_A1NIS3)

4.3.1.5.2 Information Security Awareness to All Employees

The information security team is in charge of communicating information security awareness to all employees through training and briefing sessions. In addition to briefings, seminars, training, and the like, it is observed that the information concerning information security is also posted on the bulletin board and along the walls of the main routes so that it is visible and employees may read it. It is confirmed by one of the personnel from Case 3:

> As I said earlier, starting from the first day an officer serves at this organisation, awareness programs on ICT information security will be provided. If we look at the notice boards, there are posters of government ICT security awareness (19:2_Line 31_AS3NIS1)

The CIO from Case 1 also emphasized that in her organisation, there are various methods through which all employees can be made aware of information security swiftly and immediately:

> We have an intranet. At our organisation, we have what is called a postmaster. If we want everyone to read, we will post on the postmaster. That is the first one. Secondly, we will make sure (matters related to information security) are placed on the website or portal. Alternatively, if something is serious and we want it to spread quickly, we put up posters. Alternatively, we do campaigns, ICT weeks and so on. It all depends on how serious something is, how quickly we want the thing to be communicated to everyone regularly and what we do needs to be ongoing (1:37_Line 154_AITM1)

Briefings are sometimes held in partnership with other agencies responsible for physical documents, and officials from the Chief Government Security Office (CGSO) are invited to provide security-related information encompassing all elements which are conducted physically and online:

> We once did a briefing; briefing with cooperation between my division and IT Division. We do information security briefings. Back then, we invited CGSOs and several agencies, and this involved IT Division. The division made the invitation. This briefing is related to information leakage and the latest matters (information security). That is what we do in collaboration (14:24_Line 131_A2NIS1)

4.3.1.6 Sub-Theme 6: Monitoring of Information Security Implementation

All actions pertaining to information security that are carried out by the information security team are kept under watch by top management. Although top management has mainly utilised democratic and laissez-faire methods in the administration of information security initiatives, monitoring is carried out through the presentation of information in meetings and establishing a security committee. In addition, security reports are delivered regularly and whenever an information security event occurs.

4.3.1.6.1 Presentation by the Information Security Team in Meeting/Audit Meeting

Reports on the status of information security implementation that are periodically received from the information security team are used by top management to monitor the implementation of information security. These reports will be given during meetings with the top management to gain their comments. Except for Case 1 (two (2) out of eight (8)), more than half of the participants from Case 2, Case 3 and Case 4 agreed that doing a presentation in the meeting is one of the way top management monitor information security activities. The CIO from Case 2 stated that:

> Information security matters will be presented to us during the meeting. It revolves around the presentation during the meeting, and if there are weaknesses of any security implementation, it will be highlighted (9:15_Line 113_A2TM1)

His information security personnel support the statement from the CIO:

> He (The CIO) monitors during the meeting; everything will be reported there. Suppose he wants to know how many ransomware attacks, or virus attack, the invasion occurs every month. So we will report at the meeting (11:13_90_A2IS2)

4.3.1.6.2 Establishment of Committee

Establishing an information security committee is yet another method for monitoring the implementation of information security projects. With the help of a committee like this, top management would keep a careful eye on all information security efforts and report back to JPICT for updates, as mentioned by one of the information security personnel from Case 2:

> For example, we have implemented projects initiatives (information security); we will inform JPICT. So, through the JPICT, top management can see the progress. Yes, a meeting. Progress (13:13_Line 62-64_A2IS4)

The comment that was made by one of the top management members of Case 3 is intriguing, and it justifies why there are so many committees for each information security project, despite the fact that the project will be done, and so will the committee:

> I want to share something with you. I was once asked by agencies out there, I mean, people from the industry. Why do we need a Steering Committee for Business Continuity Plan? So, I answer that the way the government works is that if we do not have a committee meeting, I mean this committee, who will monitor and drive the matter? Who wants to drive, who wants to give direction, who wants to monitor? They say that if the project is completed, the committee will be over. I told them; that we want things to be implemented continuously. That is why we insist on establishing a committee. Usually, when a project is completed, the committee will also end. However, for this matter, even during the development stage, it is still a project; it needs to be monitored all the time (20:8_Line 103_A3TM1)

One of the personnel from Case 4 shows a similar view on the establishment of a committee to monitor the implementation of information security projects as follows:

> We also have ISMS implemented. Implementing ISMS itself requires top management involvement, as we have monitoring committees which approve any security-related matters. That is why the ISMS Steering Committee will determine many things (27:1_Line 23_AS4NIS2)

4.3.1.6.3 Information Security Reports or Meeting Minutes Submitted to Top Management

The information security team's reporting on information security is presented in straightforward language, using clear analogies and concepts, and is not overly complex so that top management can comprehend what is being reported. It is essential to monitor and aid top management in decision-making for the information security team to produce reports or meeting minutes:

> Technical stuff, I rarely present it to them. I provide reports in high-level form. That is, what error occurred and the solution I have taken. Once the matter has been settled, I will let him (CIO) know. Yes, he cares. I mean, after that, he would do a follow-up with me. When I inform him it is done, he accepts. If it is not finished, he will ask me when the deadline to settle the matter is? So as long as the issue is not resolved, he will always ask and monitor (12:20_Line 217-291_A2IS3)

This monitoring practice is similar to the rest of the case studies, as supported by information security personnel of Case 4:

> ..the IT Division usually implements all reporting, and all reporting will be informed in the meeting. So, during the meeting, these things will be minuted. So based on the minutes of the meeting, our top management will monitor (22:11_Line 81_A4IS1)

In the event of significant breaches in information security, the top management will get a report on the situation. The information security team is going to figure out a solution to the problem. Once everything is done, the top management will be notified. If it turns out to be a relatively minor problem, the information security team will take care of it and let top management know that the problem has been fixed.

The comparison between all case studies shows a good agreement on how top management monitors security incidents within their respective organisation. For example, personnel from Case 2 mentioned that:

> (Incident report provided) Based on criticality, depending on the level of impact. The impact is determined based on discussions with ICT managers. One method is that we directly communicate our impact and proposed actions to top management. Another method is if the critical impact is low, we will resolve it first and then inform top management. In terms of instructions, we often ask for consent for all the actions we take. Maybe he will add a few more things for further action. For example, in the issue of ransomware, when he gets a notification from the

> MKN (National Security Council), he will ask us to prepare a notification, a notification paper for the actions taken, an announcement to all employees about the dangers, and he tells us to make reinforcements (10:17_93_A2IS1)

His colleague also stated similarly:

> If we receive any information, complaint or warning from MAMPU, the matter will be monitored. Alternatively, if we can trace it ourselves, we will perform an analysis and see the level. The security level has several levels; it has its terminology – high, medium and low levels. If it is low, we will settle the matter. We accept. We report it to top management if we see it is critical and high level. If the reporting requires immediate action, we will continue to make a minute report and notify top management directly (11:10_Line 64_A2IS2)

In the same way, one of the personnel from Case 3 quoted the following:

> There was an incident against one of the systems in the data centre. We will use the MAMPU cert. So the project group will go to the MAMPU cert group. The MAMPU cert group will first inform the CIO, and GCIO, of which incident we are dealing with and analyse and issue a report. We will see the criticality level, whether high, medium or low. If the level is high, we must complete it within a few hours based on our charter. We will look based on criticality. After that, we do hardening, and then we will report back saying the matter is done (17:6_41_A3IS1)

4.3.1.7 Summary of Information Security Governance Approach

The summary of the sub-themes derived from Theme 1 is illustrated in Figure 4.3. Overall, the approach to information security governance demonstrated by top management in the four (4) case studies is comparable.

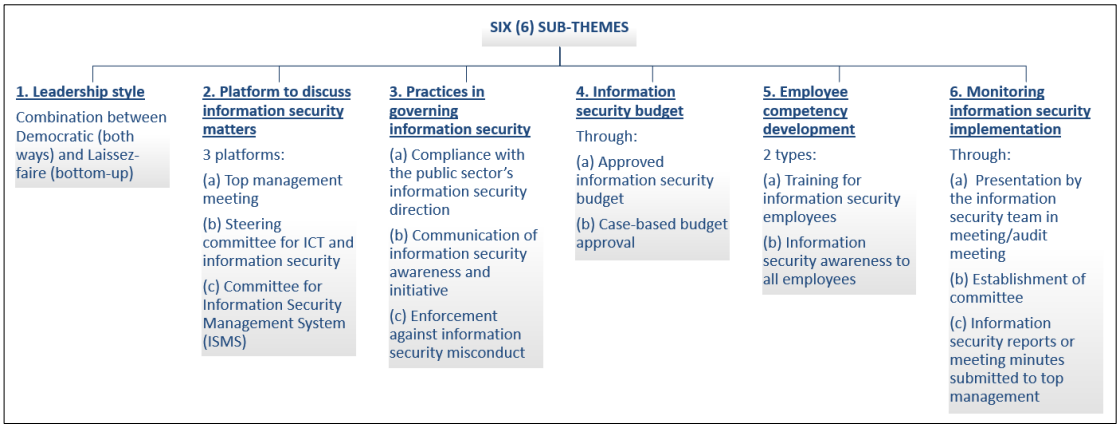


Figure 4.3: The summary of Theme 1 and its sub-themes

The researcher had anticipated this result due to the fact that the governance structure of each ministry and government agency is pretty identical. Each case study demonstrates that a consistent administrative pattern is probably the result of the impact of a central agency, such as MAMPU, which functions as a referral agency for ICT. For example, MAMPU has spearheaded the implementation of ISMS in each ministry and public sector agency as a result of the Cabinet Directive released in 2010 requiring each ministry and agency to participate in the execution of information security audits. MAMPU was a pioneer in ISMS implementation and audits and has assisted ministries and agencies in delivering training and raising awareness about the significance of this certification. As a result, MAMPU significantly impacts ICT governance in general and information security in particular among public sector organisations. This is supported by one (1) information security personnel from Case 4 who mentioned MAMPU as their referral point:

> So far, we've only referred to MAMPU. We don't hear about other agencies having the best information security since, as far as I can tell, our references in this company are just MAMPU. So, any initiative undertaken by MAMPU relating to security (information) will be seized. He was from MAMPU, just like our former boss. So, if he obtains information from MAMPU, he will request that we take advantage of all of MAMPU's information security technologies and facilities. We will participate in everything (22:39_Line 115_A4IS1)

This theme has aided the researcher in comprehending how top management oversees information security initiatives in their respective organisations, despite each

case study focusing on a distinct line of business. The information security governance structure is comparable despite having a different core business. For instance, the researcher anticipates that the leadership style of Sub-Theme 1 will vary based on the core business of ministries and agencies. Still, analysis reveals contradictory viewpoints, making it impossible to tell which leadership style is the most prevalent. Initially, it was possible that a ministry or agency where ICT was a core business would have an Authoritarian leadership style due to the educational background and the ICT-based work environment of its top management and employees. Surprisingly, though, top management and employees continue to have divergent opinions. Therefore, it may be inferred that a ministry or agency's core business does not influence the leadership style of the top management.

The degree to which the organisation relies on the IT Division to advance information security objectives is significant. When it comes to implementing information security, top management will typically consult with the IT Division, probably due to the fact that the CIO does not have a background in information security or ICT. Because of this, before a decision can be made, there is a significant amount of reliance on receiving information from the IT Division, which specializes in the field.

Based on the four (4) case studies, committees to manage information security issues have been formed and operate as planned. Budget allocation for information security is given priority. However, due to financial limits at the government level, it is essential to go through the appropriate channels and negotiate priorities with other projects. All participants are well-informed and aware of the existence of information security policies inside their organisations, as demonstrated by interviews with all respondents. According to the observations, several posters and cautions about information security are placed throughout the organisations, and this is a significant signal that every government employee has been aware of the need to preserve information security. However, there is still room for improvement, particularly in terms of the stigma that the IT Division is responsible for information security, despite the fact that the protection of information encompasses a broader scope as it involves the entirety of the organisation as the information asset is not within the purview of IT Division only.

4.3.2 Theme 2: Factors Influencing Top Management Engagement in Information Security

In this theme, the factors influencing top management engagement in information security discovered in the literature, including the Neo-Institutional Theory outlined in Chapter 2, are used to code the data during the case study. These criteria are categorised based on *multiple perspectives*, which include Technical/External (T/E), Organisational (O), and Personal (P), as well as three (3) levels of designation. The level is Top Management, Information Security Personnel, and Non-information Security Personnel. All data related to the factors impacting top management engagement in information security were retrieved and mapped against the generated codes. These data were pooled and analysed using computer-assisted techniques (Atlas.ti 22). Theme 2 is comprised of three (3) sub-themes; External, Organisational, and Personal. Figure 4.6 and Figure 4.7 summarizes the factors influencing top management engagement in information security based on case and designation, respectively. The following section describes each sub-theme in detail.

Table 4.6: Theme 2 – Factors Influencing Top Management Engagement in Information Security based on case

Sub-Theme		**Case 1**	**Case 2**	**Case 3**	**Case 4**	**Total All Cases**
External factor	▪ Regulatory forces	6/8	7/8	4/4	5/7	22/27
	Percentage (%)	*75.0*	*87.5*	*100.0*	*71.4*	*81.5*
	▪ Imitating good practice	1/8	3/8	1/4	0/7	5/27
	Percentage (%)	*12.5*	*37.5*	*25.0*	*0.0*	*18.5*

Sub-Theme		Case 1	Case 2	Case 3	Case 4	Total All Cases
	▪ Changes in security risk exposure	1/8	2/8	1/4	2/7	6/27
	Percentage (%)	*12.5*	*25.0*	*25.0*	*28.6*	*22.2*
	▪ Audit compliance	1/8	3/8	4/4	3/7	11/27
	Percentage (%)	*12.5*	*37.5*	*100.0*	*42.9*	*40.7*
Organisational factor	▪ Reputation	2/8	3/8	3/4	4/7	12/27
	Percentage (%)	*25.0*	*37.5*	*75.0*	*57.1*	*44.4*
	▪ Information security risk awareness	7/8	2/8	2/4	3/7	14/27
	Percentage (%)	*87.5*	*25.0*	*50.0*	*42.9*	*51.9*
	▪ Information security committee structure	2/8	1/8	3/4	3/7	9/27
	Percentage (%)	*25.0*	*12.5*	*75.0*	*42.9*	*33.3*
	▪ Culture	1/8	1/8	1/4	2/7	5/27
	Percentage (%)	*12.5*	*12.5*	*25.0*	*28.6*	*18.5*
Personal factor	▪ Informal education	4/8	7/8	4/4	7/7	22/27
	Percentage (%)	*50.0*	*87.5*	*100.0*	*100.0*	*81.5*
	▪ On-the-job exposure	3/8	6/8	3/4	6/7	18/27
	Percentage (%)	*37.5*	*75.0*	*75.0*	*85.7*	*66.7*
	▪ Formal education	0/8	2/8	3/4	1/7	6/27
	Percentage (%)	*0.0*	*25.0*	*75.0*	*14.3*	*22.2*

Table 4.7: Theme 2 – Factors Influencing Top Management Engagement in Information Security based on designation

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
External factor	▪ Regulatory forces	3/4	9/11	10/12	22/27
	Percentage (%)	*75.0*	*81.8*	*83.3*	*81.5*
	▪ Imitating good practice	1/4	3/11	1/12	5/27
	Percentage (%)	*25.0*	*27.3*	*8.3*	*18.5*
	▪ Changes in security risk exposure	1/4	3/11	2/12	6/27
	Percentage (%)	*25.0*	*27.3*	*16.7*	*22.2*
	▪ Audit compliance	1/4	7/11	3/12	11/27
	Percentage (%)	*25.0*	*63.6*	*25.0*	*40.7*
Organisational factor	▪ Reputation	2/4	6/11	4/12	12/27
	Percentage (%)	*50.0*	*54.5*	*33.3*	*44.4*
	▪ Information security risk awareness	2/4	5/11	7/12	14/27
	Percentage (%)	*50.0*	*45.5*	*58.3*	*51.9*
	▪ Information security committee structure	3/4	3/11	3/12	9/27
	Percentage (%)	*75.0*	*27.3*	*25.0*	*33.3*
	▪ Culture	2/4	2/11	1/12	5/27
	Percentage (%)	*50.0*	*18.2*	*8.3*	*18.5*

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
Personal factor	▪ Informal education	4/4	11/11	7/12	22/27
	Percentage (%)	*100.0*	*100.0*	*58.3*	*81.5*
	▪ On-the-job exposure	3/4	9/11	6/12	18/27
	Percentage (%)	*75.0*	*81.8*	*50.0*	*66.7*
	▪ Formal education	0/4	3/11	3/12	6/27
	Percentage (%)	*0.0*	*27.3*	*25.0*	*22.2*

4.3.2.1 Sub-Theme 1: External Factors

With reference to the Multiple Perspectives Theory adopted in this study, the perspective "T or E" is a Technical or External Factor. The sub-theme of External Factor refers to things outside the company that affect top management's engagement in managing information security activities within their organisation. These external elements include, first and foremost, external regulations, rules, laws, and other directives issued by higher authoritative bodies. Secondly, external influences involve performance and success from other ministries or government agencies, and as a result of this achievement, top management attempts to make their organisation better or at least comparable to other ministries or agencies. Following that, top management is encouraged to engage in information security in the event of ongoing issues not directly related to information security but current issues that occur outside the organisation, both domestically and internationally. Finally, external factors include compliance with external audits and accreditation from external agencies. The findings of all external influences are discussed in the following section.

4.3.2.1.1 Regulatory Forces

This sub-factor involves external regulation pressure influencing top management engagement in information security. External regulations include directives from the Cabinet, instructions, circulars, and regulations from the Chief Government Security Office (CGSO), MAMPU and other higher authoritative bodies. Regulatory Forces are the most quoted in Case 2 and 3, while for Case 1 and 4, this factor is the second and third highest quoted, respectively. 22 out of 27 participants had quoted this External Factor as one of the influencing factors of top management engagement in information security.

According to the CIO of Case 2, he stated, he will make sure that his organisation fulfils the requirements if there are instructions at the national level, a directive from the Cabinet, or instructions from the higher level of management:

> What we are doing is based on instructions at the national level. That is why we have to be precise. So, since there is a directive from the Cabinet, from the meeting to the KSU (Secretary-General to the Ministry) or the KSN (Chief-Secretary to the Government), when we get there, our responsibility as one country, one government, one public service, so we have to comply and make sure we adapt and find the way to implement it (9:13_Line 105_A2TM1)

His information security personnel supported this statement and added that buy-in from top management to implement information security initiatives would be easier if there were instructions from higher authorities.

> Yes, if the instructions come from external or from an authority, there is a level of concern by the top management of the initiative, and we will, yeah, it will be easier to get buy-in. Because the instructions are from them (external or authoritative), so it is easier for us to execute an instruction because it comes from a higher authority (10:29_Line 158_A2IS1)

Top management from Case 3 shared her experience regarding the initial implementation of ISMS and managed to get financial aid from the government because the ISMS initiative was a directive by the Cabinet.

> Because I think, if you remember, how ISMS can be moved rigorously was a decision, cabinet directive, then given a budget, RM1 million if I am not mistaken, to MKN (Malaysian National Security Council), which

> we collaborate with CyberSecurity with MAMPU, for a workshop. So that is directive from the stakeholder (20:19_Line 159_A3TM1)

She also informed that the National Cyber Security Agency (NACSA) was successfully established because the proposal for establishing the agency was brought and discussed at the Cabinet meeting and successfully obtained endorsement.

> Like the establishment of NACSA. National Cyber (Security) Agency. How can they set up that agency? They were able to set up the agency because they presented it there (cabinet meeting). They can convince the Cabinet that there is a need for a national cybersecurity agency to ensure cybersecurity in our country (20:37_Line 285_A3TM1)

The CIO from Case 1 also mentioned that any instructions from the Cabinet would become a policy, and therefore, public sector organisations should comply with the policy.

> Of course, we have, from the Cabinet, comes to the policies. So, these policies we cannot dispute. Because when this policy is formulated, there may be information or things we do not know. So, when the policy is given to the ministry or department, our responsibility is to implement it (1:54_Line 89_AITM1)

According to the statements above, the instructions and directives from the higher authority have been a factor that has made the top management treat information security efforts seriously.

4.3.2.1.2 Imitating Good Practice

Top management makes every effort to imitate other ministries or agencies, especially MAMPU, to make their organisations' information security initiatives better or comparable to others. Their tendency to compete with peer organisations influences their engagement in information security. Case 2's CIO agrees with this statement, developing a benchmark and comparing it to other ministries or agencies. If their organisation falls behind, they will strive to be the same or better.

> That is why the concept of a benchmark. We benchmark so that things will change. So, we do our best. If we are not good enough, we try to learn from the benchmark, and if we think we are good, we will not be proud. For us, if it is good, we will share how that success is achieved (9:14_Line 108_A2TM1)

Top management urges the information security team to conduct the audit and directs other agencies to do the same. One of the information security personnel from Case 2 supported the statement made by the CIO. She used her organisation's deployment of the ISMS audit as an example.

> Like the implementation of ISMS, when we accept to be implemented in our organisation, we should implement it for our CNII agency as well. Critical Information Infrastructure (CNII), right? Then they (top management) are aware of it, so they urge. We have to get it (ISMS certification) as well. Once we get (ISMS certification), they look for another agency (under this ministry) that is willing to do the same thing (13:19_Line 93_A2IS4)

There is a slight difference for Case 1, where they use examples of ministries and other agencies to look at their success in protecting their organisational information assets and learning from them, as claimed by one of the personnel:

> The reason is that sometimes when we see something happen in a government department in terms of information leakage, we will look at another place how they take care of their information. For example, in the PMO, the Prime Minister's office is tip-top in terms of confidentiality. So, we try to emulate them, but they cannot share what they use or do. However, maybe from there, we can develop those things ourselves by considering how they do. We learn from them. Let us say we have a department in the Prime Minister's Department; in terms of confidentiality, how they take care of everything, we can learn from it. And then we also have the Data Protection Department in KKMM (Ministry of Communications and Multimedia), if I am not mistaken. From there, too, we can learn (6:13_Line 188_A1NIS4)

However, this external sub-factor is not widely acknowledged and is addressed by only five (5) out of the 27 participants based on the designation.

4.3.2.1.3 Changes in Security Risk Exposure

In case of external issues, top management is encouraged to engage in information security. It's subject to domestic and international issues, so top management must be alert and careful to protect classified information. Political unrest, the government's decision to raise petrol prices, and the introduction of the Goods and Services Tax (GST) system have left the public dissatisfied and attacking government agency websites. Case 3's top management described the scenario and how they alerted other

agencies to strengthen their information security infrastructure and prepare for cyber-attacks.

> Another aspect to that, when we talk about external factors, my experience when doing incident handling with GCert, what we observe is when there are issues, current issues such as rising oil prices, so we make these factors or external issues as a reminder to other agencies to be more vigilant. For example, the increase in oil prices or the previous GST implementation, so we would, apart from the other agencies that need to focus on – the Customs (department). You will be the target of these attacks. So we have to prepare ourselves to face the attack, instead of just being ignorant and just sitting still (20:20_Line 168_A3TM1)

Following a fire incident at one of the other government agencies, information security personnel from Case 4 reported that their organisation's Disaster Recovery Center (DRC) funding allotment was successfully secured. After the incident, top management became increasingly concerned with information security measures at their organisational level.

> There is an example of a department that experienced fire during the day. The event further strengthened the reason for our organisation to hold a DRC. Because before this, when the Project Manager applied for the DRC, we did not get the budget approval. So when that happens, we see a change because there is already an example (fire incident), and the management becomes more aware of this and can get the budget approval. If not before this, every time we ask, it is not approved (23:17_Line 184_A4IS2)

Although this external issue is less prevalent among participants, with just six (6) out of 27 quoting it, it is relevant. It should be considered, prompting the top management and government agencies to be cautious and reinforce information security measures in their organisations.

4.3.2.1.4 Audit Compliance

Top management engagements in projects and information security activities can be seen in external audits involving information security in their organisations. Examples of auditing are ISMS and the Malaysian Government Performance Index (myGPI) (previously known as System Star Rating (SSR)). In myGPI, if there is a lack of any component, it will affect the organisation's rating. Also, top management is very

concerned with accreditation from external agencies such as Standard of Industrial and Research Malaysia (SIRIM), CyberSecurity Malaysia (CSM) and other international awards because such validation makes them proud of their organisational achievements. In addition, obtaining validation from external bodies will increase the organisation's trustworthiness among stakeholders. This external factor is the most quoted by Case 3, and the following is the statement by one (1) of its personnel:

> This is because this organisation (as the Central Agency) is in charge of various initiatives (ICT including information security). As a result, this type of recognition is one of the most crucial components (19:24_Line 111_AS3NIS1)

This view is also supported by one (1) of the information security personnel from Case 1:

> It is appealing to state that the organisation is of high quality (2:58_Line 436_A1IS1)

Central agencies like Case 1 and 3 need external accreditation to prove they can lead government efforts, especially in information security. The validation will boost other ministries' and agencies' trust in the central agency, especially for information security activities. Top management will always want to participate in information security projects to maintain performance and reliability, according to Case 2 personnel. However, the participant said top management's interest in information security was minimal. Information security auditing alerts management, which encourages them to implement security programmes.

> What we see is in terms of audit implementation. In the audit, there are several criteria to achieve a 5-star rating. These criteria are also beneficial. Due to these criteria, then the security of ICT seems to be given attention. Otherwise, people do not even look at ICT. So at least the criteria help in terms of alerting the management (15:34_Line 257_A2NIS2)

When the researcher inquired about the significance of an organisation receiving validation from external audit authorities, Case 4 personnel concurred and stated that such acknowledgement affects the organisation's ranking, thus increasing top management engagement in the security program:

> In terms of overall level recognition, ranking is among those that can further increase their (top management) involvement (22:36_Line 277_A4IS1)

4.3.2.2 Sub-Theme 2: Organisational Factor

The perspective "O" in the Multiple Perspective Theory is an organisational factor. All external forces (the perspective “T/E”) outside the organisation were explored in the previous sub-theme. This sub-theme is concerned with the internal organisational elements that inspire top management to participate in information security initiatives. This sub-theme consists of four (4) organisational sub-factors: Reputation, Information Security Risk Awareness, Information Security Committee Structure, and Culture. The following section contains discussions of all of these factors.

4.3.2.2.1 Reputation

Top management seeks acknowledgement in order to improve the organisation’s reputation and image. Organisations gain recognition in many ways, for example, by participating in competitions or receiving certificates or letters of appreciation from renowned international and local bodies. They “compete” with other ministries and agencies to demonstrate that their organisation is the best in terms of information asset protection. The accomplishments of central agencies such as Case 1 and 3 are critical in boosting their image as a reference point for other ministries and agencies.

When one of the top managements from Case 3 was asked about the reputation of the organisation as one of the Organisational Factors that influence top management engagement in information security initiatives, she agreed with the statement:

> If you ask me, and to the current Head of Director, yes. Indeed yes. Of course, we want to be one step ahead or many steps ahead of the other organisation (20:21_Line 166_A3TM1)

Personnel from Case 3 supported the statement made by the top management:

> Our organisation sets high standards for themselves because we are the one that puts the rating to the public sector. So, we need to improve our internal aspects to make ratings for other agencies. That means if the governance aspect that supports our strategic policies and functions is not strong, it will tarnish our image (19:10_Line 89_AS3NIS1)

The CIO from central agency Case 1 also mentioned being the best agency and how top management strives to improve their organisation's ranking in information security:

> So there is a ranking. Because of that, all Director-Generals, if possible, want to show that their agency is the best. So if the mark is 100%, they want to achieve 100% mark. So if there is a ranking, they want (the organisation) to be at least in the top 10, for example. So when he returned (to the organisation), he said, " Okay, we are currently number 20. I give you six months; we must be in the top 10 positions". So everybody, including him, works hard to achieve that (target) (1:27_Line 96_AITM1)

This issue was mentioned by nearly half of the participants (12 out of 27) across the designation, and they believe it is quite a strong motivator for top management to engage in information security.

4.3.2.2.2 Information Security Risk Awareness

Due to technology and social media, sensitive information can be easily shared with unauthorised parties. Top management engagement in information security is visible when sensitive details are intentionally or accidentally compromised, especially within the organisation. However, in the absence of security issues, they remain passive. According to one (1) information security employee from Case 4, top management will only become involved in the event of an information security problem.

> I think the issue itself. Issues that occur involving security. If there is an issue, their involvement (top management) is very high and very dominant when there is an issue. The issues that have implications for the organisation (22:35_Line 280_A4IS1)

This statement is supported by personnel from Case 1 as follows:

> If there is a case. Yes. So when there is a case, there is an issue, he (the CIO) will check where the loophole is, and then at that time, he will prioritise. If you want to ask for a budget, ask for it, that is the right time (7:8_Line 112_A1NIS5)

Furthermore, Case 1 personnel reported that if top management was ever involved in a security breach, they would take information security seriously.

> As I said earlier, it all depends on the management and their experience before becoming the boss, what they have been through such an experience (information security incident). Based on that experience, he

> will remember and apply it until he retires. However, when he works at any organisation, and everything is okay during the service, he presumes that the officers under him have taken care of everything (8:14_Line 203_A1NIS6)

As for this sub-theme, 14 out of 27 participants across the designation quoted this as one of the top management's influencing factors to engage in information security.

4.3.2.2.3 Information Security Committee Structure

Case 3's top management agreed that establishing an information committee can "force" and encourage top management to participate in information security governance.

> We were once asked, in every initiative we implement, why we always suggest there is a steering committee to monitor the (information security) initiative. However, I said it was wrong. The intention is that we want management, the management involvement in monitoring that thing (security projects) (20:23_Line 178_A3TM1)

Top management's commitment to information security is shown by their adherence to their organisations' information security committee structures. Forming committees like the ICT Steering Committee (JPICT) ensures their participation. This type of committee may be formed to encourage top management participation in information security activities, as mentioned by personnel from Case 4:

> It looks like we have set up various committee meetings. So in these committees, the CIO will be involved, so when it comes to (information security) issues, we present the paper to that committee or steering committee. I think the process will not be a problem because the CIO will be in the committee structure. So when the structure is there, I think there is no problem (27:25_Line 381_AS4NIS2)

It is standard procedure to offer roles as a chairman on a security committee to members of the top management, particularly the CIO; as a result, these individuals are obliged to fulfil the responsibilities assigned to them. Across the designation, a quarter of the 27 participants mentioned this sub-factor.

4.3.2.2.4 Culture

Top management from Case 3 mentioned that KPI is one of the pushing factors influencing top management's engagement in information security. This factor relates to an organisation's culture. Firstly, it is the competitive culture in which information security initiatives are made to be the top management's KPI. Consequently, they participate in information security to ensure that their organisations meet the KPI.

> That is why now there are so many initiatives; I once suggested for ISMS, if I am not mistaken, to be a KPI (20:37_Line 285_A3TM1)

She also added,

> Like HRMIS, we have KPIs. So all the top management tried because they were afraid of embarrassment. They are the ministries that do not achieve 100%. Then, for example, SSR. They are agencies that do not get five stars (20:37_Line 285_A3TM1)

Personnel from Case 4 also agreed with the statement made by top management of Case 3:

> KPI. It should be the organisation's KPI. KPIs are what they need. Usually, if we say we want to improve the system, security or what, it must be directly proportional to KPI. So I think the dominant factor is KPI. Organisation's KPI. Because now, everything is about KPIs. All KPIs, ministers also have KPIs (26:15_Line 166_AS4NIS1)

Second, those (top management) who speak out will have more responsibilities. Those who do not want to do extra tasks will be less engaged in security programs. Case 4 personnel reported that, because of this culture, top management is reluctant to express their opinions, conceal the fact that they are knowledgeable in security, or engage in information security activities because they do not want related responsibilities in the future.

> It is culture. If you talk a lot, then you have to do it. That is our culture. If you talk a lot, people will point at you. So in this situation, it is our culture. So culture can influence. He has to do all the things. As if he is craving power, he does so many things. After all, no one wants to do it. So people who talk a lot are the ones who need to do a lot of work. So, that is culture. So if I talk a lot, I am the one who has to do it. So the culture. Our culture influences this (26:13_Line 142_AS4NIS1)

Through the interview with the researcher, top management from Case 3 seemed to agree with the culture factor. However, she noticed such a culture no longer exists in

her organisation. Hence, she enjoyed sharing her thought, especially on information security, during the meeting with other management colleagues.

> I think it was at one point in time we attended the meeting. I felt like I could not talk. I have been through it. Because, in any organisation, there are ups and downs. I think now with the new management. We are allowed to talk. We can voice out without feeling that our views are of no value and so on. So we were given a chance, and for me, I think I enjoyed it. Sometimes when I feel like voicing my opinion, I will just do it. You have to be diplomatic, and we have to know how to do it. I think now there is freedom for this (20:25_Line 189_A3TM1)

Lastly, in security-related committees, information security is a fixed agenda in the meeting. When the topic is persistently mentioned in discussions, it may increase the top management's awareness of security issues and encourage their engagement in information security activities, as stated by Case 3's top management:

> Make it a fixed agenda in management meetings, right. If you do not have new things to present, you say no. However, the item (agenda) is there. That is one of the ways (20:23_Line 178_A3TM1)

An employee of Case 4 said that they had implemented a fixed agenda in JPICT, which appeared to be effective as the CIO became aware of and began to take additional steps to improve the organisation's information security.

> Every year, we do maintenance; automatically, the matter will be touched and presented in the meeting. So I can say our policy is dominant, and then the fixed agenda in the JPICT meeting, in the JPICT meeting is held 3 or 4 times a year. At least we will do it twice. So at the beginning of the year, we will present what we want and plan regarding ICT. What is the procurement proposal we want to implement to improve security through ISMS, SPA (security posture assessment) and other security tests – we present in the meeting. Yes, in the JPICT. So automatically, every year, we will present the same thing. So he (the CIO) will be aware every year of what activities we will do and what actions we will take to improve ICT security (24:46_Line 346_A4IS3)

On the other hand, culture is not a popular factor since only five (5) of the 27 participants mentioned it. It should be highlighted, however, that these cultural variables still exist, but they are isolated factors that occur in an organisation.

4.3.2.3 Sub-Theme 3: Personal Factor

The "P" perspective exemplifies this personal factor within the framework of the Multiple Perspective Theory. This sub-theme discusses the personal factors of top management that involve interest, passion, and formal and informal education in the field of information security, as well as the experiences of each top management member as a result of their field of work that involves information security. The sub-theme is broken down into three sub-factors: Formal Education, On-The-Job Exposure, and Informal Education, respectively. In the following paragraph, each of these underlying components will be further detailed.

4.3.2.3.1 Informal Education

How actively top management engages in information security may depend on their interest, understanding, and expertise. Participants rated Informal Education highly under the External Factor. 22 out of 27 participants agreed that informal education influences top management to engage in information security. This factor considers top management's information security interest, and the interest may have been obtained through the top management's prior experience managing various organisations, discussions with other parties, government information security directives, or other platforms. Personnel from Case 4 mentioned regarding interest in information security as follows:

> It depends on the individual. Although he is involved in ICT, even though he does not have a background (in ICT), he must develop an interest. Interest in ICT must exist. Sometimes even if he involves, when we explain the need, he still does not want to accept. Acceptance is difficult. If he does not have a background (in ICT), but he is already involved with ICT and we share many inputs with him – over time, he seems okay, and he can accept it and understand the concept of security. There are two categories of human beings. The important thing is that he must have the awareness and interest to learn, to understand the latest issues related to (information) security (22:26_Line 202_A4IS1)

This statement is also supported by her colleague, claiming that, other than interest, top management also needs a passion in executing their role in information security.

> It is his interest. His passion – that is what I saw. In terms of experience, if there is any, for example, he is lazy. Sorry, not lazy. Can I say irresponsible? Not so. However, usually, he just follows – DKICT is already there, and the security policy is in place; we follow it. Only if he has a passion for information security, he can bring, maybe he can suggest new things and so on (27:27_Line 407_AS4NIS2)

Top management that has educated themselves through self-study and reading tends to engage more in information security measures. Otherwise, they're a security initiative motivator, as reported by the CIO from Case 1:

> People who are not from the F scheme (job scheme for IT in Malaysian government) are afraid of this IT thingy. One is because they do not know. Two, they may not see the benefits. Importantly, they do not understand much. He realises only when that thing happened (information security incident). Though sometimes, the idea is simple. However, it goes a long way to make things easier, and the impact seems significant, right? It is just that; I think the CIO may be more aggressive and more hands-on with any information security initiatives he wants to implement unless the CIO himself is IT savvy. Otherwise, he is more to motivate, facilitator (1:47_Line 175_AITM1)

She also added that top management who does not understand information security might not even bother monitoring and checking the security implementation.

> The issue would be his understanding, I suppose. If he does not understand that the thing is important, he may not bother to monitor and check from time to time (1:51_Line 205_AITM1)

Implementing information security activities across the organisation requires top management's support and guidance. If top management, notably the CIO, does not have a background in ICT or information security, he must be interested in it because he leads every information security activity in the organisation. If top management is not interested in the information security project, the team will have a hard time implementing the job throughout the organisation.

4.3.2.3.2 On-The-Job Exposure

The types of roles or duties held by top management may affect their interest in information security. After a given amount of time, government servants switch ministries or agencies. Their former experiences in information security will shape their

function in the current ministry or agency. The same goes for work tasks. Top management may not have a formal academic background in information security due to the nature of work, but they must be educated and involved to fulfil their job requirements. Case 4's CIO disagreed that top management's education influences information security. She mentioned that working in the IT and information security field built her passion, which determines the amount of her participation in information security initiatives.

> For me, the educational background does not have (an impact), in my opinion. It is not the main factor determining whether you are concerned about (information) security. No. It is more when we perform the task; we look at the needs of the task. Furthermore, that task needs to have security features, so gradually, you will get involved, and you will take part to ensure that what you do is in order. I think that is more to it. More to ourselves, interest, and we want to make sure that what we do does follow the policy (21:18_Line 178_A4TM1)

The CIO further claimed that her 21 years of predominantly ICT-related job experience influenced her participation in information security initiatives within the organisation.

> Coincidentally, during the period I have been working for 21 years, I can say that 90% of my work experience is involved in matters related to information and ICT. So from there, I learned more about how we want to manage information better, maintain confidentiality, and so on. So, in fact, from there, we develop. If you are on duty for a long time, especially when you do related things, you realise that information security management is crucial (21:19_Line 192_A4TM1)

Six (6) out of eight (8) personnel from Case 2 also agreed to the fact that on-the-job experience affects the engagement of their top management in security efforts, as stated in the following statements:

> If he is from an organisation that was previously more digital or an organisation that uses technology – when we discuss an issue, he is more interested in discussing than those who have no experience. Those who have experience in the previous organisation will share, he will share his experience, and he will share views, compared to others – more to agree only. That is important. As I said earlier, if you have the experience, that is how it is (10:45_Line 244_A2IS1)

His colleague also shared her thoughts on dealing with experienced top management:

> Yes, he is different. He will concern more. For example, top management is from an agency where he greatly serves the people through the system. So when he serves the people through many systems, he understands the importance of the system, IT, security, and everything he understands. So when he came to the ministry that made this kind of policy, we did see

> the difference. He wants to know more about IT and security functions here. Because he used to work in a ministry that can serve the people through the system, about IT (13:34_Line 165_A2IS4)

18 of 27 interviewees across all scenarios could tell the difference between top management with ICT and security experience and those without such experience. Even though top management has no security background, they can participate in information security operations through on-the-job experience, and their employees perceive a different attitude from them.

4.3.2.3.3 Formal Education

An academic background in information security may offer different interpretations and opinions, which influence top management's information security engagement. This educational foundation in information security can be achieved through university years, professional training, short courses, seminars, conferences, and many others. Two (2) employees from Case 3, a central agency, said they are fortunate to have top management with ICT and security expertise.

> We are lucky because CIO herself has a security background. Plus, we in this organisation also have 3 top management, one of which is a security person. So it is easier (17:31_Line 200_A3IS1)

Another Case 3 personnel described working with top management with a background in ICT education or information security. She noted that due to their education, the top management in her company is actively involved in information security and guides their employees, as she claimed that her organisation values protecting sensitive data.

> In this organisation, it may not be a big issue. Because, as I said earlier, the CIO himself is an ICT Deputy Director-General, he has an information security background – unless he is not from the field of IT security background. Before becoming an ICT Deputy Director-General and CIO, he was an information security consultant. Then, he got promoted to her current position. So indeed, he is very concerned about any matter related to information security. So for his commitment, he is very committed. All the projects he will look at first (18:34_Line 298_A3IS2)

However, in contrast to Case 4, CIO should be filled by the F scheme top management (ICT scheme in the government sector). He said a CIO is responsible for managing

information security, but he does not have an ICT or information security (not from the F scheme), so he outsourced his responsibility to the head of the IT Division. For that reason, the organisation has trouble implementing information security measures.

> The CIO needs to be held by scheme F. This is confidential. Sometimes this deputy (the CIO) is not even from the F scheme. He came here to manage. Sometimes it is not that he does not want to know, but maybe because this is not his field, anything related to this (security), he passes back to our director, so the directive is less as this is not his field. If the CIO is the person in his field, he can give direction. More involved. All these suggestions he gave more high-level suggestions. So it is difficult for us to make a decision, for enforcement, etc. (27:20_Line 286_AS4NIS2)

This interesting opinion is rarely publicly expressed due to the delicate nature of the subject, which involves two (2) government schemes (M and F scheme). Nevertheless, several participants voiced opinions on the topic, which led to the emerging finding in Section 4.4.

4.3.2.4 Summary of Factors Influencing Top Management Engagement in Information Security

Theme 2 involved the factors influencing top management engagement in information security. This theme is important as the findings are the primary outcome of this study. Theme 2 is divided into three (3) sub-themes: External Factor, Organisational Factor, and Personal Factor. These criteria are categorised according to multiple perspectives, which include External (T/E), Organisational (O), and Personal (P), as well as three (3) levels of designation: Top Management, Information Security Personnel, and Non-information Security Personnel. Figure 4.4 depicts the summary of the sub-themes that have been derived from Theme 2.

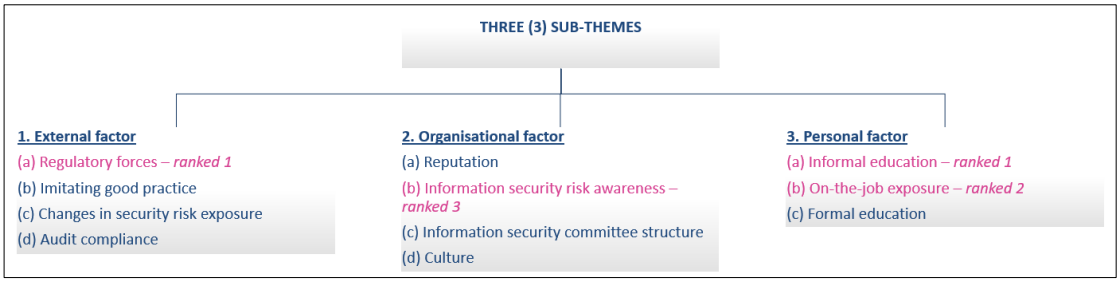


Figure 4.4: The summary of Theme 2 and its sub-themes

For the External Factor, Regulatory Forces are the sub-factor that received the most quotations from the participants across the cases where 22 out of 27 participants agreed that top management would engage more in information security initiatives when there are directives from the Cabinet, instructions, circulars, and regulations from the Chief Government Security Office (CGSO), MAMPU and other higher authoritative bodies. Audit Compliance is the second most quoted sub-factor, where 11 out of 27 participants reported that top management's involvement in information security projects could be seen when external audits occur in the organisation. Top management cares about accreditation from external agencies, including international awards, because it validates their organisational achievements and builds trust among stakeholders, including other ministries and agencies, as well as the public. When there are external directives given to ministries and agencies, it becomes the national agenda, and by hook or by crook, organisations should comprehend and execute them. Other sub-factors under the External Factor sub-theme include Changes in Security Risk Exposure and Imitating Good Practice, where 6 out of 27 and 5 out of 27 quoted the factors, respectively.

On the other hand, Organisational Factor is concerned with the internal organisational elements that inspire top management to participate in information security initiatives. This sub-theme consists of four (4) organisational sub-factors: Reputation, Information Security Risk Awareness, Information Security Committee Structure, and Culture. Among all sub-factors under this sub-theme, the sub-factor of Information Security Risk Awareness was the most quoted factor by the participants. 14 out of 27 participants mentioned that when there are events involving sensitive

details being compromised intentionally or accidentally, especially within the organisation, top management engagement in information security is started to be visible. In the absence of security issues or occurrences, however, they adopt a passive stance. This reactive approach does not come as a surprise but rather as something that was anticipated before the interview was carried out. The reactive method appears to be associated with the way that the government takes to tackle a variety of concerns, including those regarding the leakage of government information. The researcher's anticipations, which were formed before the investigation was carried out, have been shown to be correct by this finding. The Reputation sub-factor becomes the second most quoted under the Organisational Factor sub-theme, where 12 out of 27 participants claimed that top management seeks acknowledgement in order to improve the organisation's reputation and image by participating in competitions or receiving certificates or letters of appreciation from renowned international and local bodies. Therefore, in order to demonstrate their organisation is the best in terms of information asset protection, top management has the tendency to engage more in information security efforts as this can boost their image and credibility. Nine (9) out of 27 participants quoted the Information Security Committee Structure sub-factor, and five (5) out of 27 participants stated Culture as the least mentioned under Organisational Factor.

Lastly, as depicted in Table 4.8 and Figure 4.24, the Personal Factor was the most quoted factor under Informal Education. The sub-factor stated the same total number of participants who mentioned the most quoted sub-factor of Regulatory Forces under External Factor, which is 22 out of 27. Other than Informal Education, this sub-theme is broken down into two (2) more sub-factors, which are referred to as Formal Education, and On-The-Job Exposure. Top management with an adequate level of understanding of information security and educated themselves through a combination of self-study and reading tend to engage more in information security efforts. 18 out of 27 participants also quoted On-The-Job Exposure as the second most claimed quotation, followed by Formal Education, which received six (6) quotations from the overall participants.

Table 4.8: Ranking of the factors influencing top management engagement in information security from the most quoted to the less quoted

Ranking	Factor	Sub-factor	Total Quotations (out of 27 participants)
1	External	Regulatory forces	22
2	Personal	Informal education	22
3	Personal	On-the-job exposure	18
4	Organisational	Information security risk awareness	14
5	Organisational	Reputation	12
6	External	Audit compliance	11
7	Organisational	Information security committee structure	9
8	External	Changes in security risk exposure	6
9	Personal	Formal education	6
10	External	Imitating good practice	5
11	Organisational	Culture	5

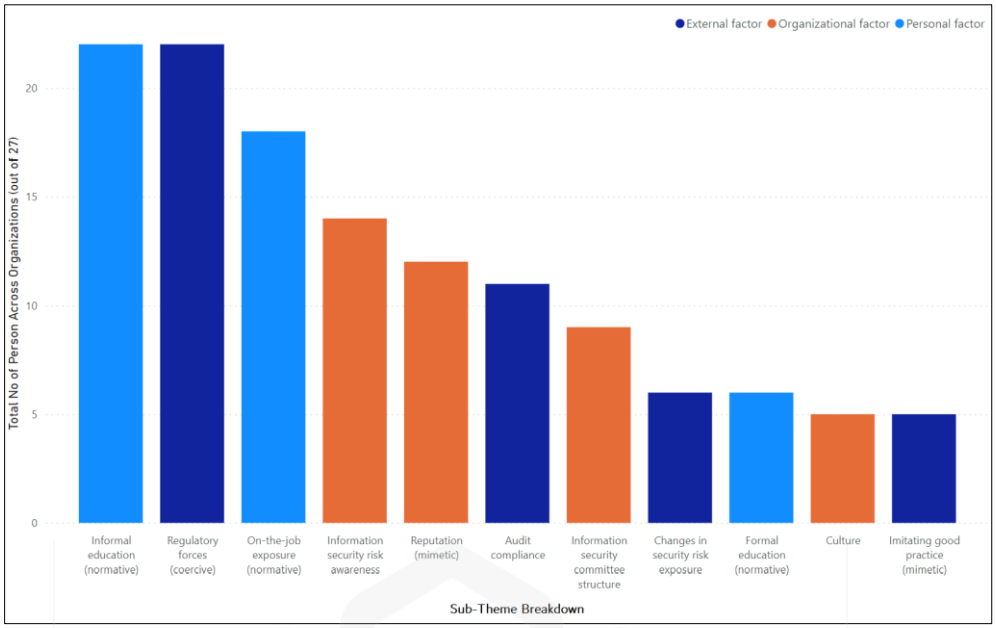


Figure 4.5: A graph indicating the ranking of factors influencing top management engagement in information security from the most quoted to the less quoted

Two (2) of the sub-factors that have received the most feedback from participants are Regulatory Forces, which go under the External Factor, and Informal Education, which falls under the Personal Factor. Both of the sub-factors recorded the same number of participants, which was 22, all of whom agreed that both of these factors were the dominating ones in determining the level to which top management was involved in information security activities in their particular organisations.

As was noted before, when external orders are given to ministries and agencies, such directives become the national agenda, and companies are obligated to comprehend and carry out those agendas. Similarly, top management who possesses an acceptable degree of understanding of information security and who has educated themselves through a combination of self-studies and reading tend to engage more in information security activities. Otherwise, they have only become a motivator in the various security activities. If there is little or no interest in the information security project, then the information security team will have a difficult time finishing the assignment because they will not have the support and engagement of the top

management. If there is little or no interest in the information security project, then the information security team will have a difficult time finishing the assignment.

On-The-Job Exposure is one more aspect of the Personal Factor that makes it into the top three (3) most frequently cited sub-factor. There was a total of 18 participants, and they agreed that this element was one of the most important factors in motivating top management to participate in information activities within their organisation. It is possible that top management does not have a formal educational background in information security because of the nature of the work they do; nonetheless, in order to fulfil their job requirements, they are still expected to be educated about and involved in information security. Because of this, it has an impact on the way they participate in information security.

Findings from this theme (the factors influencing top management engagement in information security) provided evidence of the initial research model. Validating the model includes alterations and modifications to the initial research model based on these findings and evidence. As a result, the initial research model is qualitatively validated to produce a finalised and revised model for this study.

4.3.3 Theme 3: Information Security Governance Issues

Theme 3 focuses on issues related to information security governance faced by top management and the organisation in administering and undertaking information security initiatives. This theme is intriguing since many issues about governance and the implementation of information security initiatives can be gleaned from top management and employees. Four (4) sub-themes are derived from the analysis to address research question 3 in the next section. Table 4.9 summarizes the findings for information security governance issues based on the case. On the other hand, information security governance issues based on designation are depicted in Table 4.10.

Table 4.9: Theme 3 – Information Security Governance Issues based on single case

Sub-Theme		Case 1	Case 2	Case 3	Case 4	Total All Cases
Top management constraint	▪ Limited bandwidth due to hectic schedule and various meeting agenda	2/8	3/8	0/4	0/7	5/27
	Percentage (%)	*25.0*	*37.5*	*0.0*	*0.0*	*18.5*
	▪ Inadequate knowledge and experience in information security	2/8	3/8	2/4	5/7	12/27
	Percentage (%)	*25.0*	*37.5*	*50.0*	*71.4*	*44.4*
	▪ Reactive in handling information security issues	2/8	2/8	1/4	4/7	9/27
	Percentage (%)	*25.0*	*25.0*	*25.0*	*57.1*	*33.3*
	▪ Information security is not an integral part of the organisation's business	3/8	1/8	2/4	3/7	9/27
	Percentage (%)	*37.5*	*12.5*	*50.0*	*42.9*	*33.3*
	▪ Generation gap of top management	2/8	2/8	1/4	1/7	6/27
	Percentage (%)	*25.0*	*25.0*	*25.0*	*14.3*	*22.2*

Sub-Theme		Case 1	Case 2	Case 3	Case 4	Total All Cases
Resource constraint	▪ Insufficient budget allocation	1/8	3/8	2/4	3/7	9/27
	Percentage (%)	*12.5*	*37.5*	*50.0*	*42.9*	*33.3*
	▪ Insufficient human capital	1/8	1/8	0/4	2/7	4/27
	Percentage (%)	*12.5*	*12.5*	*0.0*	*28.6*	*14.8*
Challenges in employee acceptance of information security	▪ Difficult to control staff	3/8	4/8	0/4	0/7	7/27
	Percentage (%)	*37.5*	*50.0*	*0.0*	*0.0*	*25.9*
	▪ Employee lack of information security awareness	1/8	3/8	2/4	0/7	6/27
	Percentage (%)	*12.5*	*37.5*	*50.0*	*0.0*	*22.2*
Organisation's culture	▪ Focus only on passing audit compliance	2/8	0/8	1/4	0/7	3/27
	Percentage (%)	*25.0*	*0.0*	*25.0*	*0.0*	*11.1*
	▪ The misconception of information security and ownership	0/8	0/8	2/4	4/7	6/27
	Percentage (%)	*0.0*	*0.0*	*50.0*	*57.1*	*22.2*
	▪ Difficult to change job routines	0/8	1/8	2/4	0/7	3/27
	Percentage (%)	*0.0*	*12.5*	*50.0*	*0.0*	*11.1*

Table 4.10: Theme 3 – Information Security Governance Issues based on designation

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
Top management constraint	▪ Limited bandwidth due to hectic schedule and various meeting agenda	1/4	2/11	2/12	5/27
	Percentage (%)	*25.0*	*18.2*	*16.7*	*18.5*
	▪ Inadequate knowledge and experience in information security	2/4	9/11	1/12	12/27
	Percentage (%)	*50.0*	*81.8*	*8.3*	*44.4*
	▪ Reactive in handling information security issues	1/4	5/11	3/12	9/27
	Percentage (%)	*25.0*	*45.5*	*25.0*	*33.3*
	▪ Information security is not an integral part of the organisation's business	2/4	5/11	2/12	9/27
	Percentage (%)	*50.0*	*45.5*	*16.7*	*33.3*

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
	▪ Generation gap of top management	1/4	2/11	3/12	6/27
	Percentage (%)	*25.0*	*18.2*	*25.0*	*22.2*
Resource constraint	▪ Insufficient budget allocation	4/4	3/11	2/12	9/27
	Percentage (%)	*100.0*	*27.3*	*16.7*	*33.3*
	▪ Insufficient human capital	1/4	1/11	2/12	4/27
	Percentage (%)	*25.0*	*9.1*	*16.7*	*14.8*
Challenges in employee acceptance of information security	▪ Difficult to control staff	0/4	2/11	5/12	7/27
	Percentage (%)	*0.0*	*18.2*	*41.7*	*25.9*
	▪ Employee lack of information security awareness	1/4	2/11	3/12	6/27
	Percentage (%)	*25.0*	*18.2*	*25.0*	*22.2*
Organisation's culture	▪ Focus only on passing audit compliance	1/4	0/11	2/12	3/27
	Percentage (%)	*25.0*	*0.0*	*16.7*	*11.1*
	▪ The misconception of information security and ownership	1/4	3/11	3/12	7/27
	Percentage (%)	*25.0*	*27.3*	*25.0*	*25.9*

Sub-Theme		Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
	▪ Difficult to change job routines	1/4	1/11	1/12	3/27
	Percentage (%)	*25.0*	*9.1*	*8.3*	*11.1*

4.3.3.1 Sub-Theme 1: Top Management Constraint

This sub-theme 1 revolves around top management's challenges to effectively administrate information security inside their organisations. The following section goes over all of the components of this sub-theme in detail.

4.3.3.1.1 Limited Bandwidth due to Hectic Schedule and Various Meeting Agenda

The top management has busy schedules. Meetings and events inside and outside the organisation take up most of the time. One (1) of the personnel from Case 1 supported the statement made by the CIO. The CIO quoted that:

> I think it has to do with time. Because top management is often involved in outside meetings and activities where the Director-General is not just a representative of this organisation, he sometimes must represent his boss in an outside meeting. So it took him much time (1:50_Line 199_AITM1)

Case 2's information security personnel felt sorry for the CIO, who has a lot on his plate. Even while he thinks the CIO should do a better job controlling information security in the organisation, he recognises that the CIO has a lot on his plate. The information security team handles most security concerns.

> However, in today's environment, that is the best; there is indeed a gap between ICTSO, ICT managers, and CIOs in terms of managing things. Because if we want to say top management must be 100% focused on security is not fair. ICTSO is also a CIO; at the same time, he takes care of management, management services, and development, so we realise why he cannot focus on this information security. So in the current situation, that is the most efficient, the best (10:28_Line 152_A2IS1)

4.3.3.1.2 Inadequate Knowledge and Experience in Information Security

A challenge in information security management is ensuring top management understands security. Information security governance practices are influenced by their understanding. The information security team provides input and keeps them updated on security issues. Information security personnel from Case 3 reported that:

> To me, top management level, they do not know. They do not know. They do not even know what to do. We are the ones who need to inform, need to suggest, need to advise, not the top (management) level. Because top-level does not know, all they know, they want very high-level information only (17:8_Line 47_A3IS1)

Information security personnel in Cases 1 to 4 agree on the CIO's security knowledge. Most agree that the CIO should increase their knowledge in the subject because they usually discuss information security projects with the CIO. At the government level, top management delegated information security challenges to the information security team, resulting in less involvement from top management. Personnel from Case 4 stated that:

> Knowledge. Their knowledge. As I said, they are less involved in security issues at the government level. Our government should involve the top management so that there is an increase in knowledge for them (22:34_Line 271_A4IS1)

She also added:

> I think everything is from us (the security team). When new officers at the top management level come and go, we find that sometimes when new officers come in, their awareness of information security in their previous agency is less. So those are the challenges (22:15_Line 105_A4IS1)

Personnel from Case 2 supported the opinion as follows:

> One of the challenges for us is the information gap. We want to highlight to them (top management) how severe and critical something is and also a way to suggest a solution – the information gap. Information gap involves technical matters that are among the challenges (10:52_Line 298_A2IS1)

In order to win over top management, the CIO, who attends top management meetings, must consistently stress the significance of protecting the organisation's information assets. It highlights the issues faced by the IT Division in implementing information security activities throughout the organisation, which require top management support.

4.3.3.1.3 Reactive in Handling Information Security Issues

Information security is only discussed and given significant attention after a problem or occurrence inside or outside the organisation. It was ignored until the incident; then, the action was taken. The study observed a reactive strategy typical in Malaysian public sector organisations. This matter is supported by the CIO of Case 4 as follows:

> With the SOPs that we implement, we think the implementation is already in order. So we will usually trigger this thing if there is an issue. We will look at that in detail. However, we would do, for example, if the problem occurred, we would make a precaution for the following activities. So that is how we monitor the work process (21:9_Line 79_A4TM1)

Her personnel from the information security team mentioned the same thing:

> We will discuss if there is an issue. The thing is the same as before. No news is good news. So if there is no news, the matter will be considered okay (24:21_Line 181_A4IS3)

The reactive approach is also being practised in Case 2 as reported by one (1) of the personnel:

> Regarding ICT security, if something happens, then only he will see the function. In the current mode, if there is no problem, if there is no issue, usually there is nothing that will be raised by top management (15:20_Line 155_A2NIS2)

4.3.3.1.4 Information Security is not an Integral Part of the Organisation's Business

Top management pays less attention to information security initiatives because they view it as a support function rather than a vital part of the business. Because top management lacks quantitative information to optimise security spending, security projects are assigned less relevance (monitoring, funding, etc.) than other projects. Case 3 top management claimed that IT Division must give compelling justifications so information security projects can be visible and prioritised.

> When we wanted to do this project, our organisation was the lead, and MIMOS was to develop the structure. We both contribute and complement the content. Furthermore, back then, CyberSecurity had done a survey on this project – why this project was important and how much budget was put under information security. That is why we want to emphasise (the security project) because they (top management) do not

> see the importance (of information security); that is why the budget for information security is also not prioritized (20:34_Line 42_A3TM1)

She also added that:

> I think the problem is, as you said earlier, the perception; we give less emphasis or attention to information security, it is usually placed last (20:1_Line 22_A3TM1)

An information security personnel said that security projects are less visible than other projects like system development because everyone uses a system.

> As I said earlier. Our systems are interactive, and they (top management) also use systems. So they appreciate that. So for them, systems are essential. To develop the system, you need a new server. New servers involve costs. Money is used for that purpose (buy server, etc.). For security, it is kind of passive. People hardly see it, so there is little (financial allocation) there (25:22_Line 289_A4IS4)

According to Case 4 personnel, top management knows how crucial it is to preserve information security, but as long as the current implementation has no concerns, other projects are given priority.

> If I say they do not know, they (top management) know. However, maybe they think there is something more crucial. Maybe. I think so. They know that this thing (information security) is important, and another matter is important too, but they said, oh, this thing might be more crucial. Let us do this first. As for security, so far, it is still okay (27:18_Line 269_AS4NIS2)

4.3.3.1.5 Generation Gap of Top Management

Three (3) out of four (4) top management are less tech-savvy baby boomers. When information security is discussed in a meeting, many struggles to grasp the notion. Because of this, they rely on the IT Division, information security team, or other meeting members to guide them. CIO from Case 1, a baby boomer, said that after reaching a certain level in her profession, she becomes complacent and less eager to learn new things, especially concerning information security technology.

> Generally, you become lazy to learn about IT or technology as you grow old. Because we think it is hard. The reality is that it is not difficult. Towards the end, many technologies were introduced, with only five years left to retire. We are sitting in a position where it does not matter anymore because we are already up there (1:30_Line 115_AITM1)

The same went for one of the personnel from Case 1 when he was asked how the top management coped with IT and security technology. He mentioned that:

> Technology changes every second, every second, technology changes. We take note of our top management. These are from the generation of baby boomers who used only to know typewriters. Even though I, generation X, is not very good at ICT, I also struggle to understand ICT (5:19_Line 189_A1NIS3)

Personnel from Case 4 expressed her opinion regarding her experience dealing with a different type of generation of top management:

> The age factor plays a role. In terms of knowledge related to security and ICT, younger people are more understanding and proactive. Easy for us to deal with, easy to explain scenarios, compared to the older age factor. Perhaps this is due to their lack of ICT and security exposure, then various security terms and the various systems introduced. For example, MySGRC, MyGSOC and others, it is not easy to pronounce the word. They are sometimes confused by those things. So, the age factor plays a role. The young man understood better (22:24_Line 196_A4IS1)

Case 3's personnel also claimed that an earlier generation of top management is having difficulty understanding information security and its technology.

> Yes, baby boomers. It is still difficult for them to grab this (information security). They are the TURUS (highest-level of position). Moreover, another JUSA (second highest-level of position) has to lead this ICT and security transformation (19:6_Line 65_AS3NIS1)

4.3.3.2 Sub-Theme 2: Resource Constraint

In the context of this sub-theme, resource constraint refers to two (2) different issues, namely the financial and human resources, which each organisation must contend with in order to accomplish information security efforts in the public sector in Malaysia.

4.3.3.2.1 Insufficient Budget Allocation

In all case studies, CIOs and top management agreed that insufficient budget is one of their biggest security challenges. Due to cost constraints, it's been difficult to implement information security projects that improve or add resources. Due to these limitations,

organisations must make do with the resources they have to protect their information assets, even though they cannot invest in cutting-edge security solutions. Case 3's top management said they tried to improve security, but budget constraints prevented it:

> ..However, at that time, there was a cut in the budget. To present the matter, we were sad too, because it cannot be implemented later. So there is a cost – money. As you know, security does cost money, am I right? No budget. So these are some things that the government is trying to do. People out there may not see that we have done all these things, right? All I am saying is, we try, but because of budget constraints, whatever situation, that thing may seem slow, but the effort is there (20:17_Line 146_A3TM1)

Information security personnel from Case 3 agreed with the CIO's statement:

> Like policies and so on, we can indeed do. However, in implementation wise related to security, we know that security cannot be 100% guaranteed and cannot be 100% reduced. We can only mitigate it. We cannot get a 100% guarantee that things are secure. So the implementation is a bit difficult..
> ..there are only a few issues; among them are the cost and the implementation strategy (18:10_Line 97_A3IS2)

The CIO from Case 2 also expressed the same opinion:

> First, we have constraints, such as budget constraints that cause some things; we cannot fulfil the (security) standard. That is one of the constraints. Budget (9:31_Line 215_A2TM1)

Case 3's CIO stated that, due to money constraints, they need to try in every possible way to get the budget for security implementation for her organisation:

> The main reason it has to be like that is due to resource constraints. So if we want to do something we want to do on our own, we have to work within our budget. We have to find our savings. However, if due to instructions, if we do not have enough money, we can instruct the whole JPA; okay, I need a budget from each department. Alternatively, we can go and ask from the Treasury because this is an instruction. If you want to make your own, you have to be creative and find a way to get funding for that thing (1:51_Line 215_AITM1)

4.3.3.2.2 Insufficient Human Capital

The information security team implements security initiatives organisation-wide. Due to team size, individuals without an ICT background must collaborate to meet

information security and ICT expectations. However, financial constraints are more important than human resources.

> For now, we comply with what we have. Because if we are talking about going for something bigger, we need resources. So our resources are a bit limited. It is just that we are involved in any; for example, MAMPU organises many security-related programs. So we get involved in that only. We only participate in the program. For us to handle programs for the entire organisation, I do not think so, so far (21:25_240_A4TM1)

This statement was supported by security personnel from Case 4 as follows:

> In my unit, there are only three people. So to monitor all, we lack people. I did not have time to do everything. We also take care of security, take care of the network, the network—all three things we handle on our own (25:25_Line 344_A4IS4)

4.3.3.3 Sub-Theme 3: Challenges in Employee Acceptance of Information Security

Top management is responsible for ensuring employees understand the information security's purpose. In the age of social media, top management must ensure that every employee is aware of information security to prevent accidental or intentional leaks of confidential information.

4.3.3.3.1 Difficult to Control Staff

Top management must ensure compliance with information security standards by many employees or agencies. Top management must control hundreds or thousands of employees to prevent them from leaking confidential information on social media like WhatsApp group chats, as reported by personnel from Case 1.

> Top management cares about confidentiality. Much information from this management and professional group cannot be widely disseminated. It is a secret. However, they cannot control everyone due to the large number of people. In one section here, there are about 500 people or more, if I am not mistaken. So in those 500 people, they cannot afford to monitor everyone (6:4_Line 108_A1NIS4)

His colleague from the information security team agrees with this statement:

> We are quite challenging to control if it involves social media like WhatsApp; we cannot (control)... For example, whether our officers share the secret of government information in WhatsApp (2:30_Line 215_A1IS1)

Moreover, support personnel are among those who deal with and have access to classified papers and information, as stated by personnel from Case 1:

> However, the one who arranges everything is the clerk. That is why I say clerks play crucial roles. The ones who leak much information are the clerks who serve in the technical department and operations because they are the ones who hold much information. Officers are just decision-makers, at a high level only (8:15_Line 209_A1NIS6)

Even if every employee must sign the security policy declaration form, their compliance should be checked.

> It is not easy because it is everyone's responsibility. One has read the policy, but we do not automatically control it or see if he/she has followed it. However, after he signed the DKICT, he had to obey. If he breaches (the policy), we have stated in the policy regarding the law involved. Maybe actions will be taken against him. So, he must always be aware that he has read, understood, and obeyed (13:14_Line 74_A2IS4)

4.3.3.3.2 Employee Lack of Information Security Awareness

Employees do not fully understand information security implementation, as in Case 2. After years of implementing the ISMS audit in the organisation, people are still confused with another ISO audit that no longer continues.

> Every year, we will inform the CIO JPICT that we will renew the ISMS certificate and so on. Only recently, the Head of the Director informed me that all staff understands what ISMS is. All the staff. Sometimes, when we say ISMS, people will refer to it as ISO (ISO 9001). If ISMS is referred to as ISO, the result will be the same as the previous ISOs. It will be forgotten (15:41_Line 155_A2NIS2)

Despite the documentation, top management and the information security team must ensure that the entire organisation is aware of all initiatives. Everyone, directly or indirectly, helps the organisation protect sensitive information. Case 3 personnel said they need to improve support staff's understanding of security efforts because they hold so much classified information.

> I think in terms of documentation, SOP, governance planning, and implementation – that is good. What needs to be improved is the level of understanding of the support staff related to ICT security (19:22_Line_34_AS3NIS1)

Another issue is the presumption that information security only applies to IT or that they cannot relate it to their daily tasks.

> This (information security-related matters) is rarely discussed in detail. Sub-unit, our staff does not know. Only he knows this thing needs to be kept safe. However, how serious it is and how much we have to protect, he does not know. There is no exposure related to information security. Then, in terms of the confidentiality of information, we have less exposure (7:11_Line 147_A1NIS5)

4.3.3.4 Sub-Theme 4: Organisation's Culture

The organisation's culture is comprised mainly of the perceptions of individuals within the organisation – from top management to employees regarding the significance of protecting information assets and the need to maintain an information security culture within the organisation. Audits of information security enable to determine the level of information security within an organisation, although audits of information security are regarded as cumbersome and time-consuming. Audits of information security are solely performed for certification purposes.

4.3.3.4.1 Focus Only on Passing Audit Compliance

Instead of fostering a security culture, information security measures focus on passing certification audits, as mentioned by one of the personnel in Case 1:

> Every month, we have to make security announcements. After that, in a year, we have to give a talk once or twice. We call representatives from MCMC, for example, CyberSecurity, to give talks to all staff. That is a must. Otherwise, we will not get the ISMS certificate (8:1_Line 55_A1NIS6)

Audit implementation focuses on the scope of the audit and is appreciated by a specific group of personnel, not the entire organisation. Case 3's CIO regrets that information security audits are burdensome.

> I am talking about SSR (star rating for public sector organisations), which is another aspect I regret. I regret that agencies consider this SSR and ISMS as a burden. If you feel it as a burden, then it will be difficult (20:36_Line 69_A3TM1)

4.3.3.4.2 The Misconception of Information Security and Ownership

Case 2 personnel mentioned that they tried to change top management's perception of an information security audit. Information security is often associated with the IT Division and only provides technical solutions. Nevertheless, preserving information assets is the responsibility of top management and all employees.

> In terms of the government's approach that requested all CNII agencies to implement ISMS, their initial approach led to differences in understanding, especially understanding by the management. During the early stages, we want to change top management's perception, in terms of their understanding, from what they see, this information security management system is from MAMPU, which leads the ICT. So, the implementation (ISMS) is more to data centres and portals. So, when you see it leading to ICT, people's understanding has become different. So whatever involves ISMS, they point to ICT. However, it is wrong (15:37_Line 18_A2NIS2)

Case 4 personnel, who usually associate ISMS with IT Division responsibility, supported this claim:

> For example, other departments will think this is an IT-related matter when mentioning ISMS, so they do not care. However, they need to know. For example, officers who leave the organisation and officers who just joined the organisation; create an ID, so other related departments must be aware of that. So, when we do not get cooperation from them (different departments), we find it challenging to implement (23:11_Line_143_A4IS2)

Case 3's top management faces a dilemma promoting a business continuity plan for every public sector organisation due to misperceptions of security requirements.

> In our culture, when it comes to the word ICT, anything ICT related.. for your information, when we first developed business continuity (plan), when people hear about it, they turned to ICT. When we first made PKP (business continuity plan), what was related to ICT was only the disaster recovery plan. So when I promoted this PKP, one of the participants asked why we need to do what MKN (National Security Council) does? So I answered that MKN is more about disaster management. Floods, fires involving several agencies, civilians. When we develop PKP, it is

> more to the organisation itself. Moreover, it involves the non-ICT part. We (IT Division) are not the ones in charge, just like security. I think this thing people do not appreciate, and it cannot survive because we make it very generic (20:2_Line 34_A3TM1)

The employees and top management have preconceived notions of the information security team's function because they claim that the information security team would better understand the work and would implement it. The representative must brief top management on the event. Information security initiatives are complex when management does not recognise their importance, leading to a bottom-up approach. Case 3 personnel made an interesting comment about information security understanding among non-ICT people in her organisation:

> It is like a silly question. What do you know about ICT security? When it comes to security or ICT, what do they assume? The security guards. After that, when we ask people – what do you know about ICT security? They will answer KDN (Ministry of Home Affairs), MinDef (Ministry of Defence) (17:33_Line 155_A3IS1)

4.3.3.4.3 Difficult to Change Job Routines

It is difficult to change employees' habits to comply with information security policy. They expect a slow and laborious process to ensure compliance with the regulation. Since information security is generally viewed as the responsibility of the IT Division and the information security team, obtaining collaboration from other departments to implement security initiatives is challenging. Top management must instil a culture of information security so employees do not view their work as burdensome. Case 3's CIO described the challenges she and her team faced implementing security tools in her organisation:

> I do not know where the system failed, and I think the migration also failed. It did not prove what we wanted to do, so we came out with this new DLP tool. As I said, it is a culture. If we are not passionate about appreciating the importance of something, its implementation becomes problematic. In the initial state, everyone faces challenges and disturbances during the transition period. So when we implement DLP, we have to put censors, and the agents are installed individually to get the leakage attempts. So the complaint we received at that time was that it slowed down the work process, so the staff did not agree to install the agent. Human nature. That is why there are change management terms.

> The importance of change and management. When there is a change, you need to get the buy-in. The process needs to be right for the people to accept the change (20:16_Line 144_A3TM1)

Case 2 personnel said it is hard to change a long-established routine.

> In terms of information security governance, the issue is how to change the routine. Let us say existing routines cause information leakage. So for us to change that existing routine will take time. If they implement something, we have to analyse and show the output, and then they will understand. For instance, some information should not be sent via email in the event of an incident. It should be sent by hand—things like that they cannot accept. We have to show (the implications). The reason is that the staff here have been using this method for a long time (15:33_Line 229_A2NIS2)

4.3.3.5 Summary of Information Security Governance Issues

Essentially, challenges with information security governance are classified under Theme 3. Theme 3 is divided into four (4) sub-themes, which include the constraints faced by top management in handling information security in their organisation, constraints in managing financial and labour resources, and constraints in cultivating information security culture, which includes employee acceptance of such culture. Figure 4.6 presents an overview of the sub-themes that have been created from Theme 3.

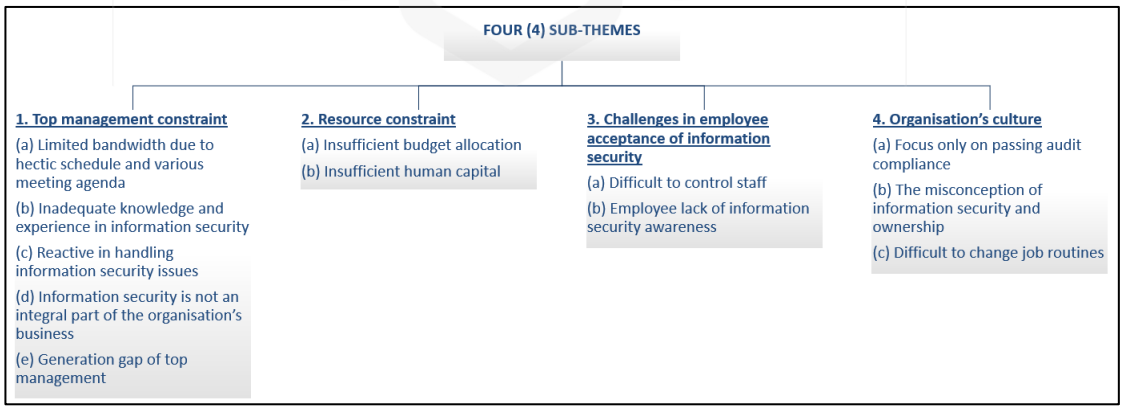


Figure 4.6: The summary of Theme 2 and its sub-themes

The CIO, who represents the organisation's top management overseeing information security activities, has a demanding workload. This is because the CIO has a primary job as a deputy secretary-general for the ministry, depending on the ministry's core business, which often includes policy, administration, and development of the organisation. Moreover, the CIO role is an integral part of the position. For example, a deputy secretary-general in charge of administration automatically becomes the ministry's CIO. The majority of CIOs do not have an IT background. Consequently, based on the findings of the interview, nine (9) out of 11 information security personnel believe that the CIO relies heavily on the IT Division, particularly the information security team, when making decisions about information security. This topic will be covered in further detail in the subsequent section.

In the public sector, it is typical for organisations to take a reactive strategy to handle issues and incidents involving information security. Nine (9) out of 27 participants concur that attention and action are only given to security incidents after they have occurred. Information security initiatives receive the least amount of attention from the organisation's top management since, in their view, information security is more of a support role than a crucial element of the organisation's operations. In addition, participants believe that older generations have trouble understanding information security and technology due partly to the generation gap.

In terms of financial constraints, this is something that every public sector organisation expects. Top management must exercise caution when spending money and selecting and prioritising projects that appear to be more critical. Information security efforts must compete for funding with other projects. Even though only four (4) out of 27 participants have mentioned the issue of labour resource restrictions, this constraint must be taken into account by the top management because of the information security team's burden to drive information security for the entire organisation. According to Table 3.7, the number of employees in Case 1 to Case 4 is 500 or more. The size of an organisation is determined by the number of employees, according to Corsten (1987). Categorization based on U.S. Small Business Administration (n.d.) as cited by Santoro & Chakrabarti (2002), firms with 500 or fewer employees are considered small, whereas firms with 500 or more employees are considered large. As

a result, all case studies are believed to belong to large firms with more than 500 employees. For this reason, top management faces significant hurdles in raising awareness and controlling employees' use of social media to share the organisation's confidential information, whether intended or unintentional.

In Case 1 to 4, the organisations already have a culture where the information security audit is more focused on acquiring certification rather than nurturing information security itself. Employees also find it tough to adapt work patterns in order to comply with the information security policy. Perceptions that the task of protecting confidential information is the sole responsibility of the IT Division also become an issue that is difficult to change.

4.4 EMERGING FINDINGS

Emerging findings are a fascinating subject that came up while analysing this study. These findings are uncovered through a study that extends beyond the research objectives and questions and demands attention and in-depth discussion. During interviews with all participants, the researcher noted that the CIO issue, which was not from ICT education and information security, was produced and remarked on by several persons from each case study. Although this is not the opinion of the majority of participants, the researcher believes some noteworthy points ought to be highlighted, as presented in Table 4.11 based on a single case and Table 4.12 based on the designation. Four (4) sub-findings related to this issue are discussed in the next sections.

Table 4.11: Emerging findings based on the single case

Emerging Findings	Case 1	Case 2	Case 3	Case 4	Total All Cases
CIO is a designation for Non-IT Job Scheme	1/8	2/8	0/4	3/7	6/27
Percentage (%)	*12.5*	*25.0*	*0.0*	*42.9*	*22.2*
The appointment of the CIO role	1/8	2/8	1/4	1/7	5/27
Percentage (%)	*12.5*	*25.0*	*25.0*	*14.3*	*18.5*
CIO is not well versed in the role and job scope as a CIO	2/8	1/8	0/4	1/7	4/27
Percentage (%)	*25.0*	*12.5*	*0.0*	*14.3*	*14.8*
CIO offloads the duties to the IT Division and information security team	4/8	4/8	2/4	5/7	15/27
Percentage (%)	*50.0*	*50.0*	*50.0*	*71.4*	*55.6*

Table 4.12: Emerging findings based on designation

Sub-Theme	Top Management	Information Security Personnel	Non-Information Security Personnel	Total All Designation
CIO is a designation for Non-IT Job Scheme	0/4	4/11	2/12	6/27
Percentage (%)	*0.0*	*36.4*	*16.7*	*22.2*
The appointment of the CIO role	4/4	1/11	0/12	5/27
Percentage (%)	*100.0*	*9.1*	*0.0*	*18.5*
CIO is not well versed in the role and job scope as a CIO	0/4	2/11	2/12	4/27
Percentage (%)	*0.0*	*18.2*	*16.7*	*14.8*
CIO offloads the duties to the IT Division and information security team	1/4	10/11	4/12	15/27
Percentage (%)	*25.0*	*90.9*	*33.3*	*55.6*

4.4.1 Sub-Finding 1: CIO is a designation for a Non-IT Job Scheme

Administrative and Diplomatic Officer (PTD; M Scheme) is the market's most exclusive Malaysian government job scheme. In current practice, only civil employees in the M scheme can be appointed to the highest position in a ministry or agency. Except in specialised agencies like medical, accounting, legal, etc., the M scheme dominates

high-level government positions. PTD come from various academic fields as well as multi-disciplinary professional experiences.

In government ministries and organisations, when an officer holds the position of Deputy Secretary-General for a specific portfolio, they preserve the CIO's position and responsibilities. That means the CIO role is not independent. It attaches to the highest management position, i.e. Deputy Secretary-General. The CIO post is not allocated to officers with IT or information security backgrounds from the F scheme, which is for the ICT area in government employment. The CIO leads the information security committee in their organisation. Most CIOs do not have a background in ICT education or information security.

Case 4 information security personnel thought the head of the IT Division should be CIO because, as an officer with ICT experience, he or she would facilitate the adoption of information security throughout their organisation:

> If in terms of leading (information security), they cannot move on their own. To move matters related to this information security, I think in here, not on their initiative. They will refer to the information management division. So, I think the information management department should take the lead. The direction (information security) is easier if it is from the ICT division itself, maybe the head of the ICT division, which needs to be a CIO. This is because they understand, and it is easy to convey something to employees. So, if there are two levels like now, we are the ones who need to explain those at the upper level, and they will sometimes go down again. So, the thing goes back and forth. I think it would be better if the ICT people themselves were the leaders in security in the agency. That is my view (22:33_Line 261_A4IS1)

Another Case 4 employee says information security direction will be easier if the CIO is from F Scheme and holds the same position as top management:

> If there is (F scheme) equivalent to them (top management in the different scheme) that can have influence, which has the same level of power as them; otherwise, we who are at the lower level can only speak. However, when the matter reaches the upper level, making that decision is not up to us. The CIO needs to be held by scheme F. This is confidential. Sometimes this deputy (CIO) is not even from the F scheme. He came here to manage. Sometimes it is not that he does not want to know, but maybe because this is not his field, anything related to this (security), he passes back to the SUB of the BPM, so the directive is less as this is not his field. If the CIO is the person in his field, then he can give direction.

> Yes. That is what I saw. So, it is difficult for us to make a decision, to do enforcement. This is because we (the F scheme) are only at the low level and cannot go up (top-level); that is our constraint. If the top management is okay, then it would be no problem (27:20_Line 284_AS4NIS2)

Case 2 personnel said the central agency planned to teach CIOs so they could carry out their obligations and help with information security directives. However, to date, there has been no development on the plan:

> Regarding the top management background, from the beginning, the central agency has said that they have a plan for CIO. Those who will be appointed as CIOs, he needs to undergo some sort of training, etc., so that he is ready to become CIOs. If the CIO has an educational background in technology, it will be easier for us to talk about direction, and so on (10:53_Line 300_A2IS1)

He stated that this predicament would continue as long as the CIO is not an ICT and information security expert.

> Indeed, that is the thing that ICTSO has to do. In fact, ICTSO assesses a security-related issue and then provides recommendations to top management on the actions that need to be taken. I think it is still the same for the future direction so long as the CIO is not skilled in technology, communication, and especially cybersecurity. Maybe one day, there will be a plan where the CIO comes from a technological background, and then only that thing will probably be a little different. That is my view (10:19_Line 105_A2IS1)

According to each of the said participants, they believe F Scheme officers should be given the CIO function and the same status as top management. Information-related issues are easier to get buy-in from other top management and can be handled more efficiently by an ICT expert.

4.4.2 Sub-Finding 2: The appointment of the CIO role is not clear

There are variations in the appointment of the CIO in each case study because this post is associated with the Deputy Secretary-General. According to Case 2 and 3, CIOs were given appointment letters for CIO roles in the form of an official letter, as claimed by the CIO from Case 2:

> Yes. It is in writing, made compulsory by the KSU himself. Not on the position itself, but there is a written appointment. Yes, it is complete,

> including the term of reference and other components. Everything is in there (9:1_Line 17_A2TM1)

The list of his CIO duties included the formal letter. With this list, the CIO will be more aware of his obligations and understand what they should do, according to Case 2's personnel:

> Together with the appointment, we will provide him with the details on the role and responsibilities. So far, it works. The CIO function correctly (12:1_Line 40_A2IS3)

In Case 1 and 4, the CIO is not formally appointed; instead, it is mentioned in the Deputy Secretary-General job description. The CIO from Case 1 and 4 said as follows respectively:

> Even though not mentioned explicitly in the list of tasks, it is understandable that as a CIO, anything to do with information technology and information systems shall become my responsibility. But in the list of tasks as the Deputy Director, it is stated that one of my roles is to be the CIO of the department. That is the arrangement (1:9_Line 31_AITM1)

> It is by default. Once you hold the position, the role comes together with it. Since ICT is under my responsibilities, automatically, I am the CIO. It is mentioned in the job list. But usually, they will inform me of this role's tasks during meetings or discussions. If you refer to someone who comes to me and tells me officially what the CIO's role is, there is no such thing. The role becomes operational in meetings (21:2_Line 41_A4TM1)

The CIO is not adequately briefed or explained their responsibilities, resulting in a problem with their role as CIO, as described in Case 2:

> Based on my observations when I first worked here. So, in the beginning, he (CIO) was a bit slow in terms of his acceptance of his duties. No one explained what his function as CIO, and then the function of the committees related to the implementation of ICT was not clearly explained (15:3_Line 51_A2NIS2)

All of these claims suggest that the CIO role is undervalued.

4.4.3 Sub-Finding 3: CIO is not well versed in the role and job scope as a CIO

In light of the fact that the CIO's function is shown to be nothing more than an "extra assignment" to the Deputy-Secretary General in the previous section, the CIO seems

unaware of their responsibilities as a CIO in an organisation. The CIO regularly asks Case 1's information security personnel about their responsibilities.

> For example, our Deputy-Secretary General, one of his roles is CIO. Sometimes when we want to meet him and discuss some matter (related to information security or ICT), he is surprised and will ask for TOR (Terms of Reference); what is the CIO's role, like that. As I said earlier, the task does not seem to be something specific on his to-do list (2:69_Line 595_A1IS1)

He also added,

> The worst happens when there is a CIO conference; he will call ICT (personnel) and ask, "Eh, what is my role? (2;67_Line 597_A1IS1)

He has never seen a CIO take on ICT and information security tasks as part of their daily duties:

> In my opinion, I think there is still no CIO who puts ICT management, especially security, in one chapter of his job on a regular basis. That is, in his to-do list (2:63_Line 547_A1IS1)

Another Case 1 personnel said the Deputy-Secretary General is focused on his primary duty and overlooks the CIO role.

> Sometimes when he is given a role as a CIO, he forgets that he is a CIO. He is more focused on his main task. The CIO is just a secondary task (6:26_Line 238_A1NIS4)

Insufficient explanation and briefing of the CIO role and ICT knowledge, particularly in information security, leads to issues elaborated in Section 4.4.3.1.

4.4.4 Sub-Finding 4: CIO offloads the duties to the IT Division and information security team

ICT advises the CIO. The information security team advises top management on security decisions. In addition to providing ICT services to the entire organisation, the IT Division ensures that top management, especially the CIO, is aware of every information security initiative, issue, and incident. If top management understands the situation, it will be easier for the information security team to get their buy-in, which is necessary to get financial support for information security projects. One (1) personnel from Case 4 shared her experience where the information team was required to attend

an information security or ICT event that required the CIO or top management, but they did not wish to participate. Top management did not prioritise it and outsourced it to the information security team:

> During the ICT engagement session, I once voiced out my opinion; next time, if it involves respondents, please invite top management or a management representative. I request that engagement sessions involve top management if there are special exercises for top management. The CIO once asked if he should attend? He said to me, "It is okay, you attend" (referring to me). The responsibility should be given directly to top management, where attendance is mandatory. The CIO must be present. That will make his job easier. Things like training, engagement, and so on (22:29_Line 227_A4IS1)

She also noted that the IT Division had become the top management's advisor on ICT and information security through its information security team:

> We are the primary advisor, advisor for ICT information security. That is, any reporting from MAMPU is directed to the IT Division. That is often the case. So, we are the ones who need to convey this to the top (management). We are the driver (22:10_Line 78_A4IS1)

Another Case 4 personnel supported the statement that the ICT Division advises top management and handles information security-related matters.

> Usually, our function is as an advisor. In addition to providing services, we are also technology advisers to top management. Sometimes something we need to implement already exists, but they do not understand the terms, and so on. So sometimes, what they convey has a specific meaning, and we may not understand it. However, once we are clear on what they mean, we know some things we need to improve. So maybe I can say here, 95% or 97% of what we have done, 3% is from the idea of management to ensure our security is at the highest level (24:3_Line 39_A4IS3)

The IT Division's information security team advises top management and gets their support. This buy-in ensures top management understands and funds an information security program. In her previous ministry, the project manager could not get top management's attention. Top management failed to understand the situation and gain their support. This shows that the information security team's justification is crucial for ensuring smooth implementation with top management's support since top management delegates responsibility to the information security team:

> Usually, when we want to get a buy-in from the top management, it depends on the project owner and how he handles the top management, how he makes top management understand a project, things like that. For

> example, if the project involves security, how does he bring the project, so that top management understands and is alert. I think that is one of the factors where the role of the project owner is to make a strategy to get buy-in. Like in my previous place at KBS (Ministry of Youth and Sports), some bosses did not know how to buy from KSU. So, during the meeting, KSU did not understand. That makes the budget application not approved (18:38_Line 271_A3IS2)

4.4.5 Summary of the Emerging Findings

These emerging findings focus on top management, specifically the CIO, who oversees all ICT initiatives in their organisation, including assessing and managing risks in information security (Hielscher et al., 2023). The role and support of top management through the CIO are vital for each information security program's success and efficiency. There are concerns about CIOs, and four (4) sub-findings classify it.

The first concern is that CIO posts attached to the Deputy Secretary-General are not filled by people with ICT and information security backgrounds. Employees, especially those directly involved in security tasks, like the information security team, believe the CIO position should go to a member of the F scheme with a background in information security and an ICT education. The CIO leads the ICT Steering Committee. A CIO must be knowledgeable about information security to raise issues and get management buy-in. This ensures that top management supports information security beyond paper. The CIO lacks information security skills. In that case, employees face challenges in getting top management's attention and support for information security initiatives, making organisation-wide implementation difficult.

Secondly, CIO appointments vary by case. The CIOs for Cases 2 and 3 have been formally appointed, but for Cases 1 and 4, the role of CIO has only been added to the job description for the current Deputy Secretary-General. Information security is a topmost concern of top management in order to protect the organisation's information assets, but the way the CIO is appointed in the ministries and agencies studied does not reflect the seriousness of top management in making information security an essential

part of the organisation's operations. This leads to the third conclusion that the CIO does not know much about the job and responsibilities.

Thirdly, these findings are tied to the problems discussed in Section 4.4.3. During interviews with participants, one issue was that the CIO lacked an academic background in ICT and information security. As a result, the CIO is not very knowledgeable about information security or his responsibilities. Therefore, a lot of weight is placed on the IT Division's information security team's input, which led to the finding.

Last but not least, the information security team has been given many CIO responsibilities. Take a situation involving information security that calls for top management but is delegated to a representative of information security. The information security team is responsible for ensuring that top management is vigilant and understands information security efforts. Top management engagement is needed to ensure the confidentiality of organisational information. Top management needs to understand and support every information security activity to keep the topic relevant. The information security team needs top management's financial support and publicity to ensure that the entire organisation cares about its initiatives.

Given the opinions of personnel, particularly information security personnel, CIOs should have academic experience in ICT. As the CIO is associated with the Deputy-Secretary General, the second-highest position in a ministry or government agency, this issue was never raised openly. Given that the M scheme holds most high-level management posts, it is unclear how much the CIO's voice will be heard at the top management level if CIO is recruited from the IT Division or F scheme. And if the CIO position is implemented as it is today, to what extent will the CIO be able to lead ICT and information security more effectively, given their knowledge of the domain? This issue, among others, is related to Malaysia's power distance and is elaborated upon in Section 5.5.

4.4.6 The Proposed Extension of RAKKSA's Competency Guidelines

The researcher found that the top management, in this case referring to the CIO, struggles to execute their roles and responsibilities in governing information security, leading to the emerging findings discussed in the previous sections. As mentioned in Section 2.5.3.2 (Chapter Two), the public sector's cyber security framework (RAKKSSA) serves as the highest reference document for ministries and agencies to establish the department's security policy. However, the RAKKSSA competency components do not include a requirement for the necessary competency for top management to govern information security in their respective organisations.

Guidelines for top management to administer information security should be included in addition to those for End-users and Implementers. This will allow the initiative taken by the government to create a comprehensive and acceptable framework at every level of government organisation, especially top management responsible for governing information security efforts in their organisations. As a result, an extension of the RAKKSSA's competency guideline has been established to address these deficiencies.

This study creates multiple perspectives mapping the top management's influencing factors on the engagement in information security from the study's findings and top management's roles and responsibilities from prior literature into a new proposed extension of RAKKSSA focusing on top management competencies. The proposed extension of RAKKSSA's top management competency is elaborated in Appendix M. This guideline shall be regularly evaluated and revised to ensure its continued applicability. Additionally, any significant changes to the information security landscape that may affect the organisation's information security shall be evaluated.

4.5 CHAPTER SUMMARY

This chapter discussed the research findings based on the data collected during the interview sessions with 27 participants from four (4) ministries and agencies of the Malaysian public sector. Analysed data were categorized into themes and sub-themes (Section 4.2). Each theme and sub-themes were discussed to have a better understanding of each case under study (Section 4.3). This chapter also highlighted the emerging findings, which is the collection of findings derived from Theme 1, 2, and 3. As a result, a significant finding has emerged, which is discussed in depth, together with the proposed guidelines for top management in RAKKSSA (Section 4.4).

CHAPTER FIVE

DISCUSSION

5.1 OVERVIEW

This chapter discusses the findings of the study presented in Chapter 4. Based on the findings gathered in Chapter 2, a field investigation is carried out to determine the similarities and differences between the literature and the findings implemented elsewhere and the research findings conducted within the scope of public sector organisations in Malaysia. At this juncture, the accomplishment of the study objectives has been determined and is covered in further detail in this chapter. Chapter 5 is organised similarly to Chapter Two and Four, which are structured according to the three (3) Research Objectives and Research Questions as described in Section 1.4 and 1.5, respectively. The organisation of Chapter 5 is illustrated in Figure 5.1.

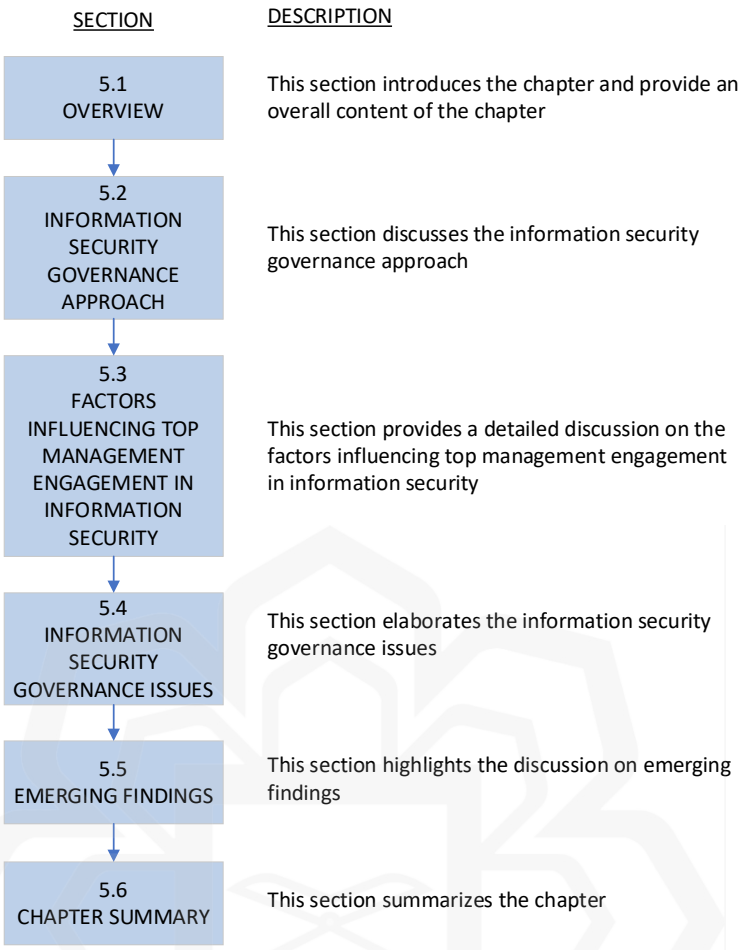


Figure 5.1: Organisation of Chapter Five

5.2 INFORMATION SECURITY GOVERNANCE APPROACH

This section tackles the first research objective, which is to investigate how top management in Malaysia's public sector governs information security in their respective organisations. Understanding the governance approach enables this study to discover the similarities and differences between previous literature and field investigation conducted in Malaysian public sector settings. This understanding leads to extracting the determinants impacting top management engagement in information security efforts and identifying the issues surrounding information security governance in the Malaysian government. The following section discusses the governance approach.

5.2.1 Top Management Leadership Style in Governing Information Security

Prior literature has discussed the significance of the role of top management in information security governance (ISG) and how a *top-down approach* will encourage employees to feel responsible for attaining the organisation's goals and ensuring its security (AlGhamdi et al., 2020). It highlights top management support as one of the critical success factors, as top management is responsible for leading information security initiatives and spreading awareness of security imports to all levels of the organisation's employees (AlGhamdi et al., 2020; Al-Izki & Weir, 2016; Dutta & McCrohan, 2002; Hu et al., 2007a; Jasperson et al., 2002; Knapp, 2005; Schinagl & Shahim, 2020; Straub, 1990; Von Solms, 2001; Young & Jordan, 2008). This is due to the fact that ISG is a part of Corporate Governance (IT Governance Institute, 2006; Von Solms & Von Solms, 2009; Warkentin & Johnston, 2008). Corporate Governance is led by the highest level of management, which is accountable for the organisation's total business functions, including IT risks. ISG is regarded to be a comprehensive approach to aligning information security policies with the organisation's objectives (AlGhamdi et al., 2020). The establishment of an ISG contributes to garnering the support of top management and including all organisation stakeholders in a top-down approach. According to the study by Hu et al. (2007), a multinational company in the USA argued that the prior bottom-up strategy was a struggle and only informal security procedures were in place. But after security reforms and practised top-down initiatives, procedures were established and accepted across the entire business; they were becoming a company-wide policy, not just a departmental one.

However, the result of the field investigation conducted in four (4) case studies representing Malaysian public sector organisations shows that the leadership style practised by the top management of the organisations in governing information security differs from the literature. This finding is evident and supported by the diverse opinions of all participants. The researcher observed that the leadership style practised in all four (4) organisations could be described as a *hybrid of Democratic (both ways) and Laissez-faire (bottom-up)*. In all organisations, the IT Division is given the autonomy to determine the implementation of information security within the organisation (Laissez-faire), but they are required to report all information related to the implementation to

the top management. The reporting requirement becomes the mechanism used by top management to oversee and controls security efforts. Nevertheless, Hu et al. (2007) stated in their research that the bottom-up approach had been a difficult journey and dilemma for the IT Division. They believed this to be the case due to the fact that the procedure for security implementation in organisations that used a bottom-up approach was established informally. This literature is in line with the problem highlighted in this study's problem statement in Chapter One, where the implementation of information security is often delegated to technical people from the IT Division, and they are responsible for shaping the security behaviour throughout the organisation with minimal or no support from the top management. If a top-down approach to security implementation is utilised, the security procedures become organisation-wide rather than department-specific policy, thus demonstrating acceptance throughout the entire organisation. However, there are times when the IT Division faces difficulties in instilling and establishing an information security culture throughout the organisation because top management views this effort as another technical matter that technical people must handle.

From another angle, since IT Division is the one who determines the information security implementation, the top management relies heavily on the IT Division for input and suggestions. As indicated in the participant's input, this dependency is also caused by the fact that most top management does not have a background in information security or ICT. This finding also explains why IT Division is given the autonomy to develop an information security policy and propose the organisation's security-related initiatives instead of the top management's directives. It can be derived that the top management's involvement entails providing feedback and endorsement on the IT Division's information security policy and approving the proposed information security activities (Democratic).

5.2.2 Platform to Discuss Information Security

Using a platform such as committees to report top-level information security agendas is one of the ideas found in a study by Kim & Kim (2015). According to the study, a

committee should recommend ways to improve information security to top management. Top management should be informed of the security committee's major agendas. This part of the information security committee's job will boost organisation-wide security.

It is observed that there are similarities between the stance expressed by Kim & Kim (2015) with the finding of this study. According to the investigation in all case studies, three (3) main platforms are employed that address all aspects of information security, namely as Top Management Meeting, the Steering Committee for ICT and Security (JPICT), and the Committee for ISMS. Since the governance structure in those case studies is identical, therefore each agency utilises the same structure. Each case study demonstrates that the use of those platforms to communicate and discuss information security agenda is probably the result of the current practice by central agencies, such as MAMPU and NACSA, which functions as referral agencies for ICT and information security, respectively. Usually, the JPICT is the highest committee that discusses ICT and information security matters; unless there is an urgent matter that requires immediate action, it will be brought to the top management meeting. It has been discovered that each of the four (4) case studies possesses a dedicated platform for the discussion of concerns and problems related to information security. They have a well-organized committee consistent with what was suggested in the prior research.

5.2.3 Top Management Practices in Governing Information Security

According to Table 2.2, one of the roles of top management in the governance of information security is to guarantee that business objectives, IT, and risk management are aligned (Whitman & Mattord, 2012b; Williams, 2001b). In addition, the top management is accountable for providing visible support and commitment to each information security initiative that is carried out within their organisation, as well as for instilling a culture of information security by setting a good example and leading by example. This responsibility goes hand in hand with the previous one. If top management is willing to provide adequate support for information security activities,

then the rest of the employees will look up to them as role models and imitate them in order to upkeep their organisation's security assets (AlGhamdi et al., 2020).

When previous works were compared to the current findings of the four (4) case studies, there were certain parallels revealed by all public sector organisations where top management practised some of the obligations stated in the previous research. Top management ensures that any information security activities are in line with the ICT strategic plan for the public sector. Each organisation's strategic plan must take into account government-developed initiatives such as RAKKSSA and Malaysia's Cyber Security Strategy 2020-2024, as described in Section 2.8.3.2 and 2.8.3.3, respectively. IT Division is responsible for establishing the organisation's strategic plan, where the division is in charge of drafting and developing organisational strategic plans before presenting them to JPICT for approval. Upon top management approval, the plan will be distributed to each agency under the organisation (if any) for reference in implementing information security activities. In contrast to the study findings by Abu-Musa (2010), the vast majority of Saudi organisations lack information security strategies, and their management has not produced policy statements about information security. The policy statements were not reviewed, updated, or approved in a few instances where such policies exist. In addition, duties and obligations related to information security are not adequately defined and articulated. Saudi organisations have no verified and effective procedures for handling information security crises and emergencies. Most respondents felt that the risk assessment procedures are insufficient to ensure compliance with applicable laws and regulations. Overall, Malaysian public sector organisations have an adequate security policy and are reviewed regularly, at least once a year. Information security roles and responsibilities are defined. If security incidents happen, processes to handle such incidents are in place.

Top management uses opportunities such as meetings, monthly gatherings and events to remind employees of the importance of preserving organisational information assets. This result further supports the idea of Siponen et al. (2014), who proposes an approach based on top management involvement and participation in information security. They argue that top management must constantly remind all employees of the importance of adhering to security policies. In this study, the support offered by the top

management is more on high-level and moral support, especially to IT Division which is responsible for implementing information security programs throughout the organisation. In order to show support for information security activities implemented by IT Division, top management will be present and give speeches on information security awareness.

According to the findings, there is also an enforcement of any security misconduct that leads to the organisation's confidential information being disclosed to individuals or other unauthorised parties. This result is in line with the study by Kaur (2016), where the scholar argues that a stricter information security policy must be implemented to instil a security culture and awareness among employees. In the case of confidential information or document leakage to unauthorised parties, the incident will be brought up at the meeting for discussion and investigation to determine what disciplinary measures should be taken against the employee. There will be periods when top management will make surprise visits to each department, as well as random spot checks. These inspections sometimes involve outside authorities, such as the Chief Government Security Office (CGSO). Warnings were given verbally and in writing, leading to more severe consequences, such as being fired or reporting the incident to the police. This finding demonstrates that organisations in the public sector in Malaysia take action on any breaches of security that an employee commit.

It has been observed that the information security strategic plan in the Malaysian public sector is relatively well organised and that regulations protecting sensitive material are in place. Top management also plays a role in communicating information security awareness to employees. There are efforts made by the government through central agencies like MAMPU and NACSA to develop a cyber security strategy and framework to deal with the information leakage issues and to preserve the CIA of government information, as discussed in Section 2.8. Furthermore, sharing information is now much easier due to the growing number of communications and social media platforms available today. Everyone has the ability to inadvertently or deliberately divulge information. For that reason, civil servants are subject to restrictions that prohibit them from disclosing confidential government information to the general public. It can be concluded that, in terms of information security strategic plans,

platforms for top management to communicate information security awareness and regulations to handle security breaches have been established and implemented in Malaysia's public sector organisations.

5.2.4 Information Security Budget

According to the top management's roles and responsibilities outlined in Table 2.2 by Whitman & Mattord (2012) dan Williams (2001), financial allocation is one of the responsibilities of top management in information security governance. This is one of the resources that top management should provide to ensure the smooth implementation of security activities within an organisation.

Most of the time, Malaysia's public sector organisations have struggled with limited financial resources. The proportion of the available financial budget that will be allocated to each ministry or agency is determined by the number of annual funds received by that ministry or agency. The budget is dependent on the planned projects and the outcomes of the preceding projects. In other words, the current year's financial allocation is based on the previous year's financial planning. This study result appears to be consistent with the responsibilities proposed by Whitman & Mattord (2012) and Williams (2001), where top management must allocate sufficient funds and resources to security initiatives. In the Malaysian public sector, there are essentially two (2) channels that are used to distribute budgets to all divisions. The first method is through a financial allocation that has been given to each division or department. The funding for the information security project is allocated to the IT Division and then divided according to the project's priority under each unit within the division. Secondly, the distribution of financial resources depends on the project's significance. This allocation takes into account the prompt execution of the ad hoc project, and the top management makes this decision. If the incident involves information security, the provision for strengthening information security will be prioritised. Therefore, the information security team's justification for requesting financial allocation must be compelling for top management to agree to fund information security projects.

Usually, budget allocation for information security is given priority. However, a Case 4 participant stated that, despite receiving the financial allocation for information security projects, it was challenging to persuade top management because they did not see the impact of the procurement. For example, the purchase of security equipment such as firewalls, which are used to ensure effective network access by targeting a variety of threats and preventing them from entering and spreading to an organisation's network. In comparison to the purchase of tangible office equipment such as photostat machines, which are used by all employees. According to statistics from Abu-Musa (2010), investments in ISG have added real value to Saudi banks and service organisations by improving reputation, maintaining market share, and increasing customer satisfaction when compared to other business types, while only one-quarter of respondents believe that ISG investments have not created or added real tangible value to their organisations. Similarly, Malaysian public sector organisations, as service providers to the people, continue to place a priority on information security initiatives. Nonetheless, the budget application requires strong justification from the information security team in order to gain buy-in and make it understandable to top management, who have little knowledge of information security or ICT. Bruin & Von Solms (2016) also mentioned the struggle between the information security team and top management to communicate ICT and security-related matters effectively, including routine cybersecurity updates and comprehensive reports. It can be seen that communication struggles between technical teams and top management are not only occurring in Malaysian public sector organisations. The justification for purchasing equipment and hardware for information security must be entirely compelling to gain top management support. Technical teams should know how to deal with and get buy-in from top management, while top management should improve their knowledge to bridge the communication gap.

5.2.5 Employee Competency Development in Information Security

According to a study by Johnston & Hale (2009), a clear high-level information security plan leads to strategies that give the organisation direction and touch on all of its parts, including its finances, research and development, marketing, human resources, and IT

resources. The organisation's policies and procedures are reflected in these strategies, which are then carried out as part of the enterprise governance process. One of the resources that top management is required to provide to employees who are involved in information security work is the opportunity to develop their competencies (Williams, 2001b). Every employee in the public sector is required to have at least seven (7) days of training. This training includes not only training specific to the job at hand but also in any other form, as well as attending speeches, seminars, and other similar events like technology update sessions. Completion of the 7-day employee training is one of the key performance indicators (KPI) for each ministry's Secretary-General. This result is in accord with the studies by Johnston & Hale (2009).

Although competency development is essential, it was discovered through interviews and document reviews that the majority of the training offered by the organisation is training that does not require financial resources, i.e. free training. Organisations offer little provision for information security training that provides employees with a professional certificate. This type of paid training is typically included in, for instance, information security or data centre acquisition contracts. As a result, only employees who actually perform information security tasks are frequently given the opportunity. Nature works in the Malaysian public sector, where employees typically do not stay in the same workplace and position for long periods, making it difficult to find a replacement who possesses the same competency as the previous employees who were groomed to be specialists in information security. As previously stated, professional training is rarely provided because it is costly and requires financial allocation from the organisation.

In terms of communicating information security awareness to all employees, the information security team is in charge of implementing information security programs and activities, including briefing sessions. A briefing session on the ministry's ICT security policy is a requirement that must be provided to all employees. Each employee who attends the briefing must sign the declaration form, which confirms that the employee attended and understood the information security team's presentation on the ICT security policy. Employees must follow the information security policy because maintaining information confidentiality is one of the Director-General's mandates.

However, the IT Division, through the information security unit, which typically consists of a limited number of employees, is responsible for implementing information security initiatives throughout the entire organisation. In addition to the information security unit's workload, obtaining the cooperation of all employees to participate in information security programs within the organisation is challenging without the support of top management. The perception is that other employees in the organisation are not serious about attending information security programs because they wish to focus on their primary responsibilities. However, if top management attends information security activities, employee attendance also increases because the presence of top management indicates the program's importance. It is challenging for the information security unit to mobilise efforts to involve information security if other employees do not take it seriously and view it as another routine activity performed by the division or department of the organisation. This is one of the issues highlighted in Section 2.7, where top management consistently views information security as a technical and operational issue (Abdul Molok et al., 2013; Williams, 2001b). Typically, the IT Division or a small security team within an organisation is tasked with managing the protection of sensitive data. This security team is responsible for ensuring that security is implemented across the entire organisation, which is impossible with minimal support from the top management. Therefore, the engagement of top management is crucial, as this is also a component of corporate governance, and top management is also responsible for ensuring that information security activities can be implemented and appreciated by all employees within the organisation.

5.2.6 Monitoring of Information Security Implementation

When it comes to the implementation of information security that is carried out by the information security unit, top management monitors all actions and tasks through the presentation of information in meetings or audit meetings, the establishment of committees, and the reading of reports or meeting minutes that are routinely submitted, as well as when information security incidents take place. The fulfilment of monitoring duty by top management in the Malaysian public sector corroborates with the idea by Williams (2001), where monitoring is one (1) of the six (6) management activities in

information security governance (ISG). The Direct-Implement-Check structure in ISG, which was suggested by Von Solms & Von Solms (2009), also includes monitoring as one of its elements.

Reports for each information security project implemented by the information security unit are distributed to top management on a regular basis and presented at meetings called JPICT, which are held once a month. These reports are presented during meetings to keep top management and all meeting attendees up to date and to solicit feedback. Participants agree that through report submission and presentation in meetings, top management monitors information security activities in their organisation.

The findings also show that top management formed committees for each information project so that top management could continue monitoring the project. This is a commendable initiative by MAMPU. As a result, as the project progresses, a committee led by top management will always be in place to monitor its progress. In addition to ensuring the project's success, top management will be kept up to date on project developments implemented by the information security unit. The formation of a committee for each project is one of the methods proposed by MAMPU to avoid the possibility of a security project failing due to a lack of monitoring from top management.

Overall, the top management of the four (4) public sector organisations followed a consistent practice to govern information security in their respective organisations. This similarity exists because these organisations use central agencies like MAMPU and NACSA as reference points when they are putting information security initiatives into action. Additionally, the majority of information security initiatives are conceived by the central agency and are delegated to other ministries or agencies for implementation and reporting project progress. Therefore, the administration and execution of each information security program that has been put into place, particularly those that involve the participation of top management, are remarkably similar to one another.

5.3 FACTORS INFLUENCING TOP MANAGEMENT ENGAGEMENT IN INFORMATION SECURITY

This section discusses one (1) of this study's main contributions and satisfies the second research objective: to determine the factors influencing top management engagement in the information security implementation within Malaysian public sector organisations.

With reference to Section 2.12.2, the researcher has mentioned the introduction of "External (E)" into the framework by merging with the "Technical (T)" perspective. The merging is proposed because the study observes zero reasonable determinants under the Technical (T) perspective based on previous literature. In addition, modifying the research framework broadens the study lens and viewpoints in exploring the top management's engagement factors in information security. However, it has also been mentioned that the finding of new factors uncovered throughout the field investigation amend the initial research model developed in Section 2.12.3. The modification to the initial model is part of validating the model as a result of multiple-case studies adopted by this research. The revised model has illustrated in Section 6.3 (Chapter 6). The discussion of the factors is elaborated in the next section.

5.3.1 Factor 1 > External

According to this study's findings, four (4) significant External Factors were mentioned by participants during the interview, and two (2) factors were derived from the initial research model (see Figure 2.11), as mentioned in Table 5.1. Two (2) external factors, *Regulatory Forces* and *Imitating Good Practice*, are consistent with previous studies, and the rest are obtained through participant interviews. Regulatory Forces is the highest-ranking factor among the four external factors listed, not only in the external factors but also in the entire factor (see Table 4.8). *Audit Compliance* is ranked second, followed by *Changes in Security Risk Exposure* and *Imitating Good Practice*. The discussion for each sub-factor is discussed in the next section.

Table 5.1: External factors influencing top management engagement derived from previous literature and field investigation

From previous literature	After field investigation (most quoted to less quoted)
(i) Regulatory forces (ii) Imitating good practice	(i) Regulatory forces (ii) Audit compliance (iii) Changes in security risk exposure (iv) Imitating good practice

5.3.1.1 External Factor > (1) Regulatory Forces

According to the findings of the interview analysis, *regulatory forces* have a high and significant impact on top management involvement in information security. This finding supports DiMaggio & Powell (1983) coercive isomorphism in Neo-Institutional Theory and is consistent with previous research by Hu et al. (2007, Johnston & Hale (2009) and Liang et al. (2007). These studies agree that regulatory force was crucial in motivating top management to engage in security initiatives so that the initiatives can be implemented throughout the organisation.

In the Malaysian Public Sector, regulatory forces are usually exerted through directives or instructions issued by the Cabinet or an Authoritative Body comprised of Central Agencies such as CGSO, MAMPU, and NACSA. Out of 27 participants, 22 agree that external regulations can influence top management involvement because external regulations are frequently on the country's national agenda and must be obeyed and implemented. For instance, every ministry and government agency must support the government's initiative to develop strategies to strengthen and address cyber security through Malaysia's Cyber Security Strategy 2020-2024 (see Section 2.8.3.1). Furthermore, it is the Prime Minister's mandate. According to one of the CIOs, any instructions from the cabinet are policy, and thus public sector organisations must follow the policy. As a result, Top Management must monitor the implementation of this strategy by their respective ministries or agencies. Similarly, the Cabinet Directive

in 2010 for ISMS implementation (see Section 2.5.3.1) has resulted in the ISMS Security Audit being implemented to this day. One of the CIOs stated that any instructions from the Cabinet would become a policy, and therefore, public sector organisations should comply with the policy. For that reason, financial aid was easy to obtain because the Cabinet's ISMS initiative was a directive.

Furthermore, one of the information security personnel mentioned that if there are instructions from an external authoritative body, it is easier to get buy-in from top management, particularly for financial provisions. One of the top managements also stated that the National Cyber Security Agency (NACSA) was successfully established because the proposal for the agency was brought and discussed at the cabinet meeting and received approval. Consequently, regulatory forces have the most significant impact on top management engagement in Malaysian public sector organisations.

5.3.1.2 External Factor > (2) Audit Compliance

Very little was found in the literature on Audit Compliance as one factor influencing top management engagement in information security. However, based on this study's findings, Audit Compliance has an impact even though this factor is placed sixth out of 11 factors in Table 4.8.

When organisations are audited externally for their information security practices, it is clear that top management is invested in the projects and activities at hand. ISMS and myGPI (formerly System Star Rating) are two examples of auditing practices used by governments. If their organisation is missing any of the myGPI components, it will have a negative effect on their overall score. In addition, top management highly values external accreditation from bodies like SIRIM, CyberSecurity Malaysia (CSM), and international awards. Central agencies like Case 1 and 3 must obtain validation from external accreditation bodies to show that their organisation is trusted to lead all government endeavours, especially in information security. The validation will increase confidence in the central agency, making it a role model for other ministries and agencies, particularly concerning information-related

activities. Stakeholder confidence in an organisation rises when it receives endorsement from credible third parties. According to a participant in Case 2, top management wants in on every information security project they can get their hands on in order to ensure the system's continued performance and dependability. Another participant claimed that the information security initiative received little attention from top management. Information security auditing is helpful because it raises management's awareness, which inspires the highest level of management to support information security initiatives.

5.3.1.3 External Factor > (3) Changes in Security Risk Exposure

Although this external issue – Changes in Security Risk Exposure is less prevalent among participants and less mentioned in previous literature, it is a significant determinant which prompts the top management and government agencies in the Malaysian public sector to be cautious and reinforce information security measures in their organisations.

In the event that there are ongoing issues outside of their organisation, top management is strongly encouraged to get involved in information security. For instance, political unrest in the country, the decision of the government to raise the price of gasoline, and the introduction of the Goods and Services Tax (GST) system, to name just a few, have left the general public dissatisfied and as a result, they have begun attacking the websites of government agencies. Because it is subject to domestic and current issues abroad, the top management must be more vigilant and careful to ensure that their classified information is not affected by incidents of this nature.

The top management of Case 3, which is a central agency, described the scenario and how they alert other agencies to fortify their information security infrastructure and prepare for potential cyberattacks. Another information security staff from Case 4 reported that their organisation successfully secured funding for its Disaster Recovery Center (DRC) after a fire incident occurred at one of the other government agencies. Following the event, top management developed a heightened sense of concern

regarding the information security measures implemented by their organisation. Even though this factor is not widely discussed in the prior research, where it was ranked eighth out of the other 11 factors (see Table 4.8), it is another significant factor derived from the findings of this study that causes top management to be involved in information governance.

5.3.1.4 External Factor > (4) Imitating Good Practice

Neo-Institutional Theory by DiMaggio & Powell (1983) defines mimetic isomorphism as organisations' response to uncertainty by replicating the activities of other organisations. According to research by Hu et al. (2007) and Liang et al. (2007), mimetic influences affect top management involvement in the security of an organisation's information system and ERP, respectively. Hu et al. (2007) contend that although there was no reported mimicking of security practices and procedures of specific companies, all three isomorphic processes (coercive, normative, and mimetic) are evident in the company and influence their managerial behaviour to some degree.

The findings of this study indicate that Imitating Good Practice has impacted top management's participation in government information security initiatives. However, as shown in Table 4.8, Imitating Good Practice factor ranked tenth out of eleven determinants discovered during a field investigation of four (4) Malaysian public sector organisations. Although this factor influences top management's involvement in information security, it is not as significant as the Regulatory Forces factor. As stated in Section 2.8.1, two (2) central agencies, MAMPU and NACSA, serve as information security reference agencies. Top management makes every effort to imitate the central agencies and other ministries to make their organisations' information security initiatives superior or comparable to those of other organisations. They encourage the information security team to conduct the audit to implement the same to compete with peer organisations or learn from the success of other ministers and agencies in protecting their organisation's information assets. Overall, this result is consistent with the study by Hu et al. (2007), which found that, although this factor is less significant,

it still influences the top management's efforts to drive information security within their organisation.

5.3.2 Factor 2 > Organisational

According to the findings of this study, four (4) significant Organisational Factors were mentioned by interview participants, and one (1) factor was derived from the initial research model (see Figure 2.10.3), as shown in Table 5.2. Two (2) organisational factors, *Information Security Committee Structure* and *Reputation*, are consistent with previous research, and the rest are obtained through participant interviews. Based on Table 4.8, *Information Security Risk Awareness* is ranked fourth among Organisation Factors, followed by *Reputation* in fifth, *Information Security Committee Structure* in seventh, and *Culture* in eleventh. The following section goes over each sub-factor in detail.

Table 5.2: Organisational factors influencing top management engagement derived from previous literature and field investigation

From previous literature	**After field investigation (most quoted to less quoted)**
(i) Organisation's condition (ii) Organisation's size (iii) Work patterns and practices (iii) Reputation	(i) Information security risk awareness (ii) Reputation (iii) Information security committee structure (iv) Culture

5.3.2.1 Organisational Factor > (1) Information Security Risk Awareness

According to the findings of this study, Information Security Risk Awareness has significantly influenced the engagement of top management in information security.

Based on Table 4.8, this factor ranked fourth. It indicates that four (4) case studies of Malaysian public sector organisations practice *a reactive approach* in dealing with information security incidents.

Because of advancements in technology and the widespread use of social media, sensitive information can be easily compromised and distributed to individuals who are not authorised to receive it. These incidents can occur for a variety of reasons, including theft, hacking, and human error. This can have serious consequences. When there are incidents involving sensitive information being compromised intentionally or accidentally, particularly within Malaysian public sector organisations, top management engagement in information security begins to become visible. On the other hand, when there are no threats or incidents involving security, top management takes a more passive stance. One of the participants mentioned that the top management would only become involved in the event that there is a problem with the information security of the organisation. In addition, other participants reported that if top management has ever been involved in an organisation that had a security breach, they are likely to take information security concerns very seriously. This was reported by participants who had previously participated in an organisation that had experienced a security breach.

Many organisations have ineffective data protection, and it is due to how firms plan their information security programmes. In reviewing the past literature, Johnston & Hale (2009) argues many organisations also plan information security reactively, and their asset protection strategies are based on perimeter incidents. In a similar vein, Knapp et al. (2006) and Veiga et al. (2020) suggest that organisations can transition from a reactive style of security management to a much more proactive one when addressing information security incidents. A study by Guo (2013) mentioned that top executives decide an organisation's IT strategy and budget. How much money is spent here depends on how important executives view IT and security. The term "top management support" leads to a "supporting" role. When top management plays a supporting role, security management becomes an IT problem instead of a business problem. With this method, top management takes a passive, reactive approach to security issues, meaning they only act when breaches occur.

Malaysian public sector organisations opt for a straightforward and reactive approach to addressing information security issues. According to the research that has been done in the past, this approach has been taken not only by case studies in the public sector in Malaysia but also by a significant number of other organisations both in and outside of Malaysia. Many organisations consider the current level of security protection to be in good condition as long as there are no information security incidents. However, this assumption changes once an incident does take place. Naturally, this kind of mindset needs to be changed because if an incident of information security occurs and affects the business operation of an organisation, the repercussions are severe and difficult to rectify.

5.3.2.2 Organisational Factor > (2) Reputation

The findings of previous research indicate that the impact of security incidents has an effect on the *reputation and image* of the organisation. Organisations must safeguard their information and assets in order to maintain their worth and reputation. The failure of an organisation's information security procedures can have a direct influence and inflict significant damage to the organisation's reputation and finances (Abu-Musa, 2010; Ahlan et al., 2015; AlGhamdi et al., 2020; IT Governance Institute, 2006; Nellis, 2003). Therefore, organisations must safeguard their information assets because they are vital and directly impact the overall reputation of the organisation. Therefore, the findings of previous research indicate that the impact of security incidents has an effect on the reputation and image of the organisation.

According to the findings of this study, Reputation is the fifth most influential factor in the participation of top management in information security, as listed in Table 4.8. As a Malaysian government entity, reputation is critical in instilling trust in the public. In terms of information security, a strong reputation contributes to public confidence and reliability. As a result, government agencies are particularly concerned about their organisations' reputations, as government agencies possess and retain the country's critical data, including people's data. According to the interviews, top management desires recognition in order to strengthen the organisation's reputation and

image. One participant of Case 3's top management said that Reputation directly impacted her involvement, and over half of the participants believed that reputation is a powerful motivator for their top management to engage in information security activities. According to the participants, organisations acquire recognition in a variety of ways, such as by participating in competitions or receiving awards or letters of praise from prestigious international and local organisations. They "compete" with other ministries and agencies to prove that their organisation provides the best protection for information assets. Case 1 and Case 3 achievements as central agencies are crucial for enhancing their reputation as a point of reference for other ministries and agencies. This is among the reasons why the information governance approach in all four (4) case studies is identical, as the government agencies mimic the style of central agencies. Also, central agencies are responsible for becoming pioneers and providing guidelines to other ministries and agencies regarding information security implementation. Therefore, Malaysian public sector organisations safeguard their information assets because they are vital and directly impact their reputation as a whole.

5.3.2.3 Organisational Factor > (3) Information Security Committee Structure

Kim & Kim (2015) expressed a viewpoint regarding utilising committees as a platform for reporting information security agendas to the top management. According to the study's findings, a committee should be used to provide top management with recommendations regarding things that should be done to ensure continuous improvement of information security. No matter what kind of committee it is, the top management ought to be informed about the major agendas concerning security. This aspect of the job of the information security committee will assist in bolstering information security throughout the entire organisation.

Through committee to conduct information security matters can "force" and encourage top management to participate in information security governance in their organisation. Consistent with the literature, this research found that the top management from the interview agreed to establish a committee to allow their engagement in information security. It demonstrates the level of commitment these individuals have to

information security matters because top management is required to adhere to the information security committee structure in their respective organisations. Forming committees like the Information and Communications Technology Steering Committee (JPICT) in Malaysian public sector organisations allow their participation in information security activities. Furthermore, it is standard practice to offer members of the top management, in particular the CIO, roles as chairman of a security committee. Therefore, these individuals are obligated to fulfil the responsibilities that have been assigned to them. As a result of the involvement of the top management in the information security committee, the instructions and the implementation of the information security program are able to be expanded to encompass the entire organisation. In light of this, the formation of a committee is one approach that can be taken to compel the direct participation of top management in information security.

5.3.2.4 Organisational Factor > (4) Culture

According to a study by Veiga et al. (2020), some ideas for creating a good information security culture relate to rewarding employees, capacity building, general meetings, purposeful development and motivation and implementing consequences for non-compliance. However, security, education, training and awareness (SETA) were listed mostly as the resolution to create a good security culture.

Culture is a unique and diverse factor that varies from organisation to organisation. In the context of this study, culture relates to how an organisation's work practices in the public sector influence top management's participation in information security initiatives. In this study, Culture was found to influence top management engagement in information security even though this factor is not popular and ranked last in the overall ranking factors shown in Table 4.8.

During the field investigation that was carried out in four (4) public sector organisations, one of the top managements mentioned that KPI is one of the pushing factors that influence top management's engagement in information security. Firstly, the competitive culture drives top management to make information security initiatives

their key performance indicator (KPI). They do not want to fall behind other organisations and strive to be the best at all times. As a result, they participate in information security activities to guarantee that their organisations will achieve the KPI. Secondly, there is a culture in the Malaysian public sector in which those (top management) who consistently voice their opinions are given additional responsibilities and leadership roles. Therefore, those who wish to avoid taking on additional responsibilities are likely to remain reticent and disengaged from any security programme. Participants also reported that as a direct result of this culture, top management is more hesitant to express their opinions, conceal the fact that they are knowledgeable in the area of security, or engage in information security activities because they do not wish to be burdened with more responsibilities in the future. Participants also reported that this culture has made top management more reluctant to participate in information security activities. On the other hand, she observed that such a culture was no longer present in her organisation with the recent change of management members. She argued that the meeting with the other management colleagues was an enjoyable opportunity to share her thoughts, particularly concerning information security. Last but not least, information security is always a topic when it comes to meetings and committees dealing with security, such as JPICT. The participants believe that when the subject is repeatedly brought up in discussions, it may increase the top management's awareness of security issues, encouraging their engagement in information security activities. Participants also mentioned that they had implemented a regular or fixed agenda in JPICT, which appeared to be effective as the CIO became aware of information security matters and began to take additional steps to improve the organisation's security. This is consistent with the findings of Abu-Musa (2010)'s study, in which the majority of respondents confirmed that ISG is always a priority for the board of directors in their respective organisations. Therefore, the study recommended that the boards of directors of Saudi organisations pay more attention to ISG issues and make them a regular, important agenda item. For that reason, incorporating information security into a regular agenda ensures that it always receives the attention of top management and serves as one of the motivating factors for top management to become involved.

To summarize, in Malaysian public sector organisations, the three (3) aspects of their culture that can influence top management's involvement in information security are meeting the KPI, having a culture of speaking up, and ensuring that an information security agenda is fixed in meetings and committees. This culture promotes top management involvement in their organisations' information security programs and initiatives.

5.3.3 Factor 3 > Personal

According to the findings of this study, four (4) significant Personal Factors were mentioned by interview participants, whereas three (3) factors were similar to the previous initial research model (see Figure 2.11), as shown in Table 5.3. Based on Table 4.8, *Formal Education* is ranked ninth among Personal Factors, followed by *On-the-job Exposure* in third and *Informal Education* in second. The following section goes over each sub-factor in detail.

Table 5.3: Personal factors influencing top management engagement derived from previous literature and field investigation

From previous literature	**After field investigation (most quoted to less quoted)**
(i) Age (ii) Formal education (iii) On-the-job exposure (iv) Informal education (v) Tenure in company	(i) Informal education (ii) On-the-job exposure (iii) Formal education

5.3.3.1 Personal Factor > (1) Informal Education

According to Katsikas (2000), individuals appointed with information systems security responsibilities had received formal or informal information systems security education. In addition to requiring formal education, top management without a background in security or ICT must expand their *informal education* to the knowledge of information security to manage their organisations. Informal education in information security is gained from the individual's desire to increase their understanding of information security through self-reading and exploration. According to the summary of top management roles and responsibilities by Whitman & Mattord (2012) and Williams (2001) (see Table 2.2), top management should have a solid understanding of information security to perform their roles in information security governance. Niekerk & Von Solms (2010) argue that security knowledge can influence users' security behaviour. When users in an organisation are aware of and educated on the standards that govern how they manage information security, they are more likely to act accordingly (Ogbanufe, 2021).

In the case of Malaysian public sector organisations, Informal Education received a very high quotation from participants and is ranked second (see Table 4.8). 22 out of 27 participants agreed that Informal Education is the most influencing factor for the top management to engage with information security initiatives. The level of interest, understanding, and competency that top management has on the subject matter may affect how actively they engage in information security activities. This factor considers situations in which top management is interested in information security. This interest may have been gained through the top management member's prior experience leading various organisations, communicating with other peer professionals, and executing information security directives issued by the government or from other relevant platforms. Another participant also supports this statement, claiming that, other than interest, top management also needs a passion for executing their role in information security. Top management with an adequate understanding of information security and who educated themselves through a combination of self-study and reading tend to engage more in information security efforts. Otherwise, they have just become a motivator in security initiatives. The participant also added that top management who

does not understand information security might not even bother monitoring and checking the security implementation. From the findings, if top management, specifically the CIO, does not have an educational background in ICT or information security, he must be interested in information security because he leads every information security initiative within the organisation. If there is little or no interest in the information security project, then the information security team will have a tough time completing the assignment since they will not have support and engagement from the top management. Implementing information security initiatives throughout the organisation does not solely fall on a small information security team's shoulder but necessitates top management's understanding and support to make it work.

5.3.3.2 Personal Factor > (2) On-the-job Exposure

Work experience, or in the context of this study, *on-the-job exposure*, shapes behaviour, resulting in top management's engagement in information security. According to Safa et al. (2015), experience with information security entails familiarity with information security occurrences and the abilities and knowledge to prevent, manage, and mitigate the risk of information security events. On-the-job exposure is achieved from experience in prior workplaces or current work assignments, which helps to mould behaviour and ultimately leads to the involvement of top management in information security. Through the experience of developing and using IT, the management learned how important information security is and how important it is to have an information security strategy (Chang & Ho, 2006b). Albrechtsen (2007) argues that the lack of experience in information security is the most significant issue in regard to the role of users in information security work, as experience helps to develop appropriate behaviour in a fast-changing environment.

The finding of this study indicates that on-the-job exposure has a significant impact on the engagement of top management in information security. Based on Table 4.8, this factor is ranked third among all the factors. The level of engagement of top management in information security may be affected by the types of jobs or responsibilities they have held in the organisation. It is a practice in the Malaysian

public sector to exercise work rotation and job reshuffle, where employees are required to move to another department within the same ministry or agency or move from one ministry or agency to another after a certain period. Their role in the information security efforts of the present ministry or agency will be shaped by the experiences they gathered while serving in the organisations they have worked for in the past. At the same time, for top management holding CIO roles who do not have a background in ICT education or information security, exposure to information security is gained through their previous work experience in private or public sector organisations. In addition, they have been exposed to information security throughout their careers and have attended courses and training on information security themes.

The same principle applies to tasks at work. Due to the nature of their work, most top management may not have a formal academic background in information security; yet, they are still required to be knowledgeable about and involved in information security in order to fulfil their job obligations. According to the CIO of Case 4, she did not agree that education background influences top management's engagement in information security. However, she claimed that the work nature related to IT and information security reignites her interest and determines the level of top management participation. The CIO further claimed that her 21 years of predominantly ICT-related job experience influenced her participation in information security initiatives within the organisation. Six (6) out of eight (8) personnel from Case 2 also agreed to the fact that on-the-job experience affects the engagement of their top management in security efforts. About half of the interviewees across all case studies were able to discern a difference between working with top management with extensive ICT and information security experience and those without such experience. Even if certain top management lacks a security background, they are able to participate in information security operations due to their work experience. The participants asserted that through observation, they were able to determine which members of top management possessed appropriate experience in information security based on their participation in information security activities and their attitude toward information security.

5.3.3.3 Personal Factor > (3) Formal Education

Prior research contends that learning the necessary skills and competencies and education can lead to expertise in information security (Katsikas, 2000; Peltier, 2005; Tsohou et al., 2008). Organisations should pay particular attention to security education since it is a critical approach to enlightening users about their security roles and responsibilities and promoting appropriate behaviour among them (Cavusoglu et al., 2015). For instance, Safa et al. (2015) argue that active participation in information security workshops effectively influenced users' awareness and behaviour. From this literature, it is clear that in the field of information security, education is critical for producing knowledge and creating awareness of their duties and responsibilities.

Even though formal education is ranked ninth (see Table 4.8), the result of this study indicates that formal education foundation in information security gained from academic institutions may yield varied interpretations and views towards information security among top management. Formal knowledge of information security can also be acquired through several other sources, such as professional training, short courses, seminars, conference, and many others. This factor does affect the top management engagement in information security. According to two (2) personnel from Case 3, a central agency, they claimed that they are fortunate because they have top management that is well-versed in information security due to the fact that they come from an ICT and security academic background. Due to a lack of interest on the part of technical personnel to effectively articulate security strategies, many organisations struggle to convey information security issues to top management. On the other hand, top management with substantial expertise in the field of information security, or at least a background in ICT education, actively participates in every information security activity and guides their employees genuinely. This is due to the top management's extensive information security knowledge, making governance efficient and straightforward.

However, in contrast to the viewpoint of personnel at Case 4, he thinks it should be entrusted to top management from the F scheme to fill the position of CIO (ICT scheme in the government sector). He stated that a CIO was responsible for managing

every information security endeavour; however, as the CIO did not have an ICT or information security (or not from the F scheme) academic background, he outsourced his responsibility to the director of the IT division. As a direct consequence of this, the organisation has a number of difficulties when attempting to implement information security measures. Through this factor, the researcher has uncovered an emerging finding concerning participants' perceptions of the credibility of a particular job scheme in the Malaysian public sector to lead information security within an organisation. This opinion is interesting, yet, it is rarely publicly articulated due to the delicate nature of this subject matter, which is caused by the involvement of two (2) different government schemes (M and F scheme). This topic is discussed further in Section 5.5.

5.4 INFORMATION SECURITY GOVERNANCE ISSUES

This part addresses the third research objective, which is to identify the issues linked to information security governance that are faced by top management in organisations that fall within Malaysia's public sector. This topic is noteworthy since, during the interview process in four (4) Malaysian public sector organisations, quite a number of concerns surrounding security governance and the implementation of information security initiatives were brought up. The following section expands on the issues raised.

5.4.1 Issue 1 > Top Management Constraint

The schedules of top management are often hectic. Most of the time is taken up by the administration of various things, such as meetings and activities inside and outside the organisation. An information security personnel from Case 2 expressed his understanding towards the top management, specifically the CIO, *who has many things on his plate.* Even though he believes that the CIO could do better in governing information security in the organisation, the effort shown by the CIO is sufficient to the fact that the CIO has a lot of things to handle. Consequently, most concerns regarding information security are referred to the information security team to manage.

One of the issues in information security governance is *top management's inadequate knowledge and experience in information security and how to ensure that top management has a proper understanding of information security.* According to Chang & Ho (2006), top management's IT competence may affect their attitudes toward implementing security standards and willingness to serve in leadership roles within information security management. They may also have more confidence in steering proactive security behaviours. Their comprehension of information security influences the governance patterns they use in information security. However, from this study's findings, it can be seen that top management relies on the information security team to provide input and keep them updated on matters related to information security. Information security personnel from Case 1 to Case 4 have a common view about the knowledge the CIO possesses regarding information security. The vast majority of them are of the opinion that the CIO ought to advance their level of expertise in the area. This is because, most of the time, they communicate with the CIO regarding information security projects within their organisation. At the government level, the top management delegates the responsibility for information security issues to the information security team, which results in reduced involvement from the top management in information security concerns. This is contrary to what was stated in the previous literature stated that despite all employees having information security responsibilities, the accountability for managing information security risks and their countermeasures lies on the shoulder of the organisation's top management (Fazlida & Said, 2015; Khoo et al., 2010b; Williams, 2001b). In order to win over the support of top management, it is imperative that the CIO, who is also a member of top management meetings, constantly discuss the importance of protecting the organisation's information assets. It includes highlighting the challenges faced by the IT Division in implementing information security efforts throughout the organisation, which require full support and commitment from the top management. Top management needs to be forced to accept the ultimate responsibility to ensure that information security is aligned with the overall business objectives and mission (Budzak, 2016; Von Solms, 2001; Williams, 2001b).

Based on the researcher's observations and analysis findings, the researcher found that a *reactive approach* was a common and regular practice in Malaysian public

sector organisations. In the Malaysian public sector, information security is brought up for discussion and given special attention in the event that a problem or incident arises either inside or outside of the organisation. It was disregarded until the incident occurred, at which point it was taken into consideration and action was taken. The reactive approach practised by the Malaysian public sector is highlighted by a study from Johnston & Hale (2009) which stated that many organisations plan information security reactively, and their asset protection strategies are based on perimeter incidents. One of the reasons for this reactive approach is highlighted by Guo (2013), where in many cases, the function of top management is minimised to that of a supporting role, which is frequently referred to as "top management support". The top management of an organisation plays a supporting role, which turns security management into an information technology challenge rather than a business one.

This is in opposition to the concept of ISG proposed by the (IT Governance Institute, 2006; Von Solms & Von Solms, 2009; Warkentin & Johnston, 2008), where information security matters need to be integral but transparent in enterprise governance. Putting the information security issues as nothing more than an operational component of IT resulting the top management taking a passive and reactive stance toward security issues, meaning that they try to do something only after security breaches have already occurred. This scenario exists in Malaysian public sector organisations where *initiatives pertaining to information security receive the least amount of attention from the top management because of their perspective that information security is more of a support function for the organisation rather than an essential component of its operations.* As a result of the lack of quantitative information that top management needs to have in order to optimise security investments, security projects are given less importance (monitoring, budget, etc.) than projects in other disciplines. This scenario supported the literature by Whitman & Mattord (2012), which argues that top management is reluctant to invest in more effective information security solutions as it would appear to be a waste of funding. Top management from Case 3 reported that IT Division needs to make strong justification so that projects under information security could be visible and thus prioritised by the top management. An information security personnel said that security projects are less visible than other projects like system development because everyone uses a system. According to

personnel of Case 4, top management is aware of how vital it is to maintain information security; yet, as long as the current implementation does not have any issues, other initiatives that top management considers to be more important are given priority.

Three (3) out of four (4) top management come from *the baby boomer generation, with less experience with various forms of technology*. When information security concerns are brought up in a meeting, they have difficulty understanding the concept and giving it some thought. Because of this, they rely on the IT Division, information security team, or other members of the meeting to help guide them through the decision-making process. CIO from Case 1, who is also a baby boomer generation, stated that, after reaching a certain level in her career, she becomes complacent and less interested to learn new things, particularly about the technology for information security. As a consequence of this, the information security governance Malaysian public sector has a greater propensity to stick with the status quo and carry on with the practices that have been established rather than adopting a more proactive and innovative strategy.

5.4.2 Issue 2 > Resource Constraint

In the context of information security efforts in the public sector in Malaysia, the term "resource constraint" refers to two (2) distinct issues, namely the financial and human resources, which each organisation must contend with in order to accomplish its goals.

Not only in public sector organisations in Malaysia but also in organisations all over the world, the *lack of available financial resources* has traditionally been a source of struggle. According to research by Gupta & Hammond (2005), the lack of available funds was cited as the primary obstacle faced by 49% of organisations in the United Kingdom when it came to implementing computer security measures. Research on information systems security, on the other hand, indicates that limitations on an organisation’s financial resources are the second most crucial factor in determining whether or not an organisation is ready to implement a technology (Gupta & Hammond, 2005; Karyda et al., 2006; Tejay & Barton, 2013; Wang et al., 2009).

In Malaysian public sector organisations, the amount of yearly funds acquired by each ministry or agency determines how much of the available financial budget will be distributed to them. There are basically two (2) different processes that are used in order to distribute financial budgets among all of the divisions that make up their various organisations. The first way is through a financial allotment that has been made for each department. The budget is contingent on the planned projects and the results of the projects that came before them. Second, the distribution of financial resources is contingent on the project's significance. This allotment takes into account the prompt execution of the ad hoc project.

In this study, all CIOs and top management agreed that an inadequate budget is one of the most significant challenges they face when attempting to provide the most effective security solutions for their organisations. Implementing information security projects that involve either increasing the quality of already existing resources or investing in new ones due to cost constraints has been difficult. Because of these constraints, organisations have little choice but to make do with the resources available to them to maintain the security of their information assets, even though they cannot invest in the most cutting-edge security solutions. In order to maintain the security of their information assets, organisations must make do with the resources they have available to them. The top management from Case 3 mentioned that despite the fact that efforts had been made to improve the level of security protection, it could not be implemented due to limitations in the budget. The CIO of Case 3 explained that due to the organisation's limited financial resources, they need to try everything in their power to obtain the budget for the implementation of security measures for their company. This is also due to departments within an organisation requiring more immediate attention.

Even though only four (4) out of 27 participants have mentioned the issue of *lack of human resources,* this constraint must be taken into account by the top management in the Malaysian public sector because of the information security team's burden to drive information security for the entire organisation. Based on this study's findings, the information security team must ensure that all information security initiatives are effectively implemented across the organisation. Sometimes, in Case 2,

for example, in order to meet the requirements for information security and ICT, members of the team who do not have a background in ICT will need to work together, despite the fact that this is not their area of expertise. However, the issue of human resources is not nearly as pressing as the financial constraints that each Malaysian public sector organisation must contend with.

5.4.3 Issue 3 > Challenges in Employee Acceptance of Information Security

In this day and age of social media, top management in Malaysian public sector organisations also faces the issue of ensuring that the security awareness of the information reaches every employee to prevent any confidential information from being leaked either intentionally or unintentionally on social media. Top management is responsible for guaranteeing that employees can comprehend the purpose of implementing information security within their organisation. This issue is emphasized by Hu et al. (2007), stating that the challenges stemmed from the need to educate employees across all organisational levels and departments on the significance of information systems security in order to ensure that they would be willing to accept the repercussions of their actions when it came to the handling of sensitive data. Top management must ensure that a large number of employees or agencies are in constant compliance with information security standards.

However, according to the study's findings, *it is challenging for top management to control hundreds or thousands of employees* and ensure they do not leak the organisation's confidential information on social media like WhatsApp group chats, as reported by personnel from Case 1. Even if every employee is required to sign the security policy declaration form, the degree to which that person complies with the requirements of the form is something that can be questioned and should be checked. Moreover, support personnel are among those who deal with and have access to classified papers and information, as stated by personnel from Case 1. Support staff, such as clerks and administrative assistants, who are tasked with protecting a file room containing confidential government files and documents, employment records, and salary information, or a car driver who overhears their boss's conversation while the

boss is travelling in their vehicle, are examples of potential risks. Despite the fact that officials are frequently the focal point of information awareness efforts and are more exposed to such information security, support staff have a low awareness of information security and are commonly overlooked. The researcher believes that personalised security education, training, or awareness should be provided to each hierarchical level or division in public sector organisations so that they can relate information security to their daily tasks and the nature of their work.

Additionally, based on the findings, there is a problem in which *employees do not fully understand the implementation of initiatives relating to information security,* like the one mentioned by personnel in Case 2. He stated that after years of implementing the ISMS audit in the organisation, members of the organisation are still confused with another ISO audit (ISO 9001 Quality Management System) which was introduced earlier in the public sector organisations. This is due to the fact that security audits, such as ISMS, are usually implemented and appreciated by personnel within the certification scope. In Malaysian public sector organisations, the scope of ISMS certification is frequently focused on the data centre operating under the IT Division. ISMS implementation is also less prevalent, and as a result, ISMS certification is not popular and well-known within the organisation. There is also a common misconception that ISMS is closely connected to ICT and, as a result, falls under the jurisdiction of the IT Division. However, if the ISMS certification gains the attention and support of top management and its scope is expanded to include departments other than the IT division, the researcher believes the audit can be implemented and appreciated by the entire organisation.

Everyone contributes in some way, whether directly or indirectly, to the success of the organisation's efforts to preserve sensitive information. One of the issues that top management and the information security team have is ensuring that the entire organisation is aware of all initiatives despite having all the documentation in place. Personnel from Case 3 believed there is a need to improve the level of understanding, especially among support staff, regarding the security efforts as they hold so much classified information and documents. There is also the false assumption that information security only applies to departments that deal with ICT (Rai & Chukwuma,

2017) or that people do not understand how information security relates to their daily work. This perception needs to shift to make it possible for information security initiatives to be broadly implemented across the entire organisation.

5.4.4 Issue 4 > Organisation's Culture

For this study, the Malaysian public sector organisation's culture is comprised mainly of the perceptions of individuals within the organisation – from top management to employees regarding the significance of protecting information assets and the need to maintain an information security culture within the organisation. Information security audits enable weighing the level of information security within an organisation by evaluating, identifying and rectifying security loopholes. However, information security audits are cumbersome, time-consuming, and performed for certification purposes. Instead of concentrating on inculcating a security culture in the organisation, *the information security measures that have been established are geared around passing certification audits,* as mentioned by one of the personnel in Case 1. In Malaysian public sector organisations, audit implementation only focuses on the scope that falls under the audit's purview and is appreciated by a particular group of personnel within the audit scope, not something that needs to be practised in the entire organisation. Information security audits are also considered burdensome, especially to the implementer, as the top management of Case 3 expressed her regret over the perception.

In addition to the compliance work that needs to be done, according to the observations made by the researcher, an ISMS audit in Malaysian public organisations requires the development, implementation, and ongoing maintenance of a significant amount of documented information. This information includes policies, procedures, and standard operating procedures (SOPs). This security audit appears to be additional work on top of the implementer's regular responsibilities, particularly for the information security team. Furthermore, it is human nature to dislike being questioned, and the audit causes the implementer to feel uneasy because it gives the impression that the auditor is looking for flaws and asking about their work, even though the auditor's job is to help

improve the process and help strengthen any information security loopholes that the organisation may have overlooked.

Personnel from Case 2 stated that they tried to change the perception of the top management regarding implementing an information security audit. There is *a misconception that information security is usually associated with the IT Division* since they consider information security as a technical solution. However, preserving information assets requires top management and all employees' responsibilities and making it a culture. This claim is also supported by personnel from Case 4, where people usually relate ISMS with IT Division responsibility. For instance, the top management from Case 3 faces a dilemma in promoting the need for a business continuity plan for every public sector organisation due to the misperception of security requirements. The top management and employees have a preconceived notion of the information security team's function. For example, in the event where the presence of top management is required, they instruct the representative from the information security team to attend on their behalf. The representative must give the top management a detailed description of the event. The rationale is that the information security team has a greater understanding of the work and would be the one to carry it out later. Information security initiatives are complex to realise when management does not appreciate the matter and its relevance, which lead to a bottom-up approach. This finding is comparable to research by Hu et al. (2007) in one of their case studies, where information systems security was always the responsibility of specific personnel in the IT department. Top management, business managers at various levels, and even IT staff who were not directly responsible for security all had the same expectation that security personnel were doing all possible to implement foolproof security technologies and procedures. From the literature and this study's findings, it appears that information security concerns are not among the top priorities of an organisation's top management, and changing this image will be difficult.

It is challenging to alter individuals' habits inside an organisation to comply with information security policy. They anticipate that the workload will increase in order to ensure compliance with the regulation, resulting in a slow and laborious process. This perception is similar to what Hu et al. (2007) did in their study, where they found that

a similar perception underlies the comments of other interviewees who expressed ambivalent or unfavourable attitudes toward security protocols due to their belief that protocols impacted work routines. It becomes a challenge for top management to instil a culture of information security so that employees no longer perceive their work as burdensome. It is difficult to change the routine when the method has been implemented for a long time in the organisation. There is a perception that information security is generally the duty of the IT Division and the information security team; thus, obtaining collaboration from other departments to implement information security initiatives throughout the organisation is tricky. However, the responsibility for maintaining information security should be split among the various departments that make up an organisation, which requires interaction, cooperation, and commitment from employees in all parts of the business (Allen & Westby, 2007). In order to ensure the continued viability and safety of their organisations, information security issues need to be given the same level of attention as other strategic concerns at the governance level (Allen, 2005; Lidster & Rahman, 2018; Whitman & Mattord, 2012a). The researcher believes the process would be more straightforward if there were instructions and support from higher-level management.

5.5 DISCUSSION ON THE EMERGING FINDINGS

Administrative and Diplomatic Officer (PTD; M Scheme) is the market's most elite, sought-after government employment scheme. PTD usually occupies the highest positions in the public sector. In the current practice, only the civil servants within the M scheme could have the opportunity to be appointed to the highest position within the ministry or agency. It is pretty uncommon to find other than the M scheme dominating the high-level position in the government except in specialized agencies such as medical, accounting, legal, *et cetera*. PTD comes from various academic domains such as literature, business, law, finance, and many more, as well as from multi-disciplinary working experiences.

As for the current practice in Malaysian government ministries and agencies, when an officer holds the position of Deputy Secretary-General for a specific portfolio,

they will keep the CIO's position and responsibilities. That means the CIO position is not independent. It attaches to the top management position, i.e., Deputy Secretary-General. The CIO position is not dedicated to officers with IT or information security backgrounds, precisely, the F scheme, which is a scheme for the ICT domain in government employment. In 3 of 4 case studies involved, the CIO leads the organisation's information security committee (JPICT). Another case study is led by a higher position which is Secretary-General. Nonetheless, *all CIOs and top management do not have a background in information security or at least in ICT.* Employees, particularly those directly involved in security tasks, such as the information security team, believe that it would be more appropriate if the CIO position is given to a member of the F scheme with a background in information security or ICT. Furthermore, if the CIO comes from F Scheme and at the same time holds the same hierarchical level as top management, information security direction would be easier. This ensures that the importance of information security is not just on paper but is translated into top management's engagement. It will ease the adoption of information security throughout their organisation, and information security direction will be clearer and can be conducted more efficiently by a security expert. If the CIOs and top management are knowledgeable in ICT, particularly in information security, buy-in from other top management will also easily obtain every time information security matters are brought up in meetings. There is a plan where the central agency intended to give CIOs training so that they would be prepared to carry out their responsibilities and would also assist with information security directives. To date, however, there have been no developments about the plan. However, this situation would continue so long as the CIO is not higher-level management with a background in ICT and information security.

The appointment of the CIO role varies from case study to case study due to the fact that this CIO post is associated with the position of Deputy Secretary-General. The CIOs for Case 2 and 3 have been formally appointed. CIOs were given appointment letters for CIO roles in the form of official letters. The formal letter was also included on the accompanying list along with the duties he was expected to perform as a CIO. At the very least, with this list of chores, the CIO will be more aware of his obligations and understand what they should be doing. In contrast, for Case 1 and 4, the CIO does not receive a formal letter of appointment; instead, the role of the CIO is one of the tasks

stated in the Deputy Secretary-General's job description. The CIO does not receive an adequate briefing or explanation of their responsibilities, which results in an acceptance problem about their function as CIO. From all of these assertions, it is possible to deduce that the CIO role is only another position that is given less weight. Although information security is one of the primary concerns of top management in order to guarantee that the organisation's information assets are always protected, the manner in which the appointment of the CIO is carried out in the ministries and under study does not reflect the seriousness of top management in bringing information security to an important agenda as an essential component of the organisation's operations. This leads to the next argument, which is that the CIO is not very knowledgeable about the job and responsibilities that come with being a CIO.

In light of the fact that the function of the CIO is shown to be nothing more than an "extra assignment" to the Deputy-Secretary General, *CIO seems not to comprehend and is unaware of the responsibilities that they are expected to do in their role as a CIO in an organisation.* According to an information security personnel from Case 1, their CIO regularly inquires about his responsibilities with the information security team. He also noted that he has never seen the CIO take on chores involving ICT and information security as part of their day-to-day responsibilities. Another personnel, also from Case 1, stated that the Deputy-Secretary General is more focused on his primary duty and overlooks the role of the CIO of the organisation. These findings are intricately connected to the problems that are discussed in Section 4.4.3.1. One of the issues that came up during the interviews with the participants is the fact that, again, the CIOs do not come from an information security nor ICT academic background. As a result, the CIO is not very knowledgeable about information security or his responsibilities as CIO. As a result, a significant amount of weight is placed on the input provided by the IT Division's information security team, which led to the subsequent argument.

ICT Division takes on the role of advisor to the CIO to assist top management in making well-informed decisions regarding information security. This means the information security team has been given many of the CIO's responsibilities. One of the participants shared her experience where the information team was required to attend an information security or ICT event that needed the CIO's or top management's

participation. However, the CIO did not prioritise it and refused to participate. Instead, the CIO outsourced this responsibility to the information security team. IT Division had become not only the advisor to the top management but also the driver in matters pertaining to ICT and information security through the information security team. The information security team bears a significant amount of responsibility for ensuring that top management is continually vigilant and has a solid comprehension of the requirements of information security efforts. Not only the IT Division is responsible, through the information security team, is accountable for providing ICT services to the entirety of the organisation, but they are also responsible for ensuring that top management, particularly the CIO, is aware of every information security initiative, issue, and incident that occurs within their organisation. If the top management understands the situation, it will be much easier for the information security team to obtain buy-in from them, which is essential to get financial support for information security projects. The justification from the information security team is crucial for guaranteeing that the implementation of information security can be carried out smoothly with the support of top management. One of the forms of support that the information security team requires from top management is to receive a financial allocation for information security initiatives. Furthermore, publicity shown by top management allows the entire organisation to be aware of the initiatives carried out by the information security team.

These emerging findings indicate that the top management, in this case referring to the CIO, is struggling to execute their roles and responsibilities in governing information security. Therefore, this study synthesizes previous literature and emerging findings by mapping the factors influencing top management engagement in information security to their respective roles and responsibilities. The mapping results in a proposed extension of RAKKSSA centred on top management competencies, as illustrated in Appendix M. This extension ensures that the customized information security policy made by the ministries and public sector agencies of Malaysia will have better coverage in the competency component, which now covers top management, end-user, and the implementer.

Given the opinions of personnel, particularly information security personnel, it is recommended that CIOs be selected from officers with an academic experience in the ICT domain. However, as the CIO is also the Deputy-Secretary General, which is the second-highest position in a ministry or government agency, this issue becomes tricky and hence is not raised. There is a dilemma regarding the extent to which the CIO's voice will be heard at the top management level if CIOs are recruited from the IT Division or F scheme, given that the F scheme does not hold high-level management posts. And if the CIO position is implemented as it is today, to what extent will the CIO be able to drive ICT and information security more effectively, given that they have insufficient knowledge of the domain? This issue, other than rooted in the various Schemes in the public sector, is directly tied to Malaysia's power distance.

According to the Hofstede Index, Malaysia has one of the highest power distances in the world, which indicates that people accept hierarchical order without more justification (Hofstede Insights, n.d.). Hofstede Index defined Power Distance as,

> the extent to which the less powerful members of institutions and organisations within a country expect and accept that power is distributed unequally

This dimension deals with the inequality of persons in societies. It expresses the culture's attitude toward disparities. Malaysia ranks very high on this dimension (100), which suggests people accept a hierarchical order in which everyone has a place and needs no more reason. Hierarchy in an organisation is perceived as reflecting fundamental inequities, centralization is popular, subordinates expect to be told what to do, and the ideal leader is an autocrat. Challenges to leadership are also not welcome. Therefore, those in lower-level positions may be afraid to speak up, or their thoughts may not be considered.

In random comparison to the other 12 countries, the power distance in Malaysia records a very high number (see Figure 5.2, Figure 5.3, Figure 5.4, Figure 5.5). According to Hofstede, a high Power Distance is directly associated with the autocratic or authoritarian leadership style as referred to in this study.

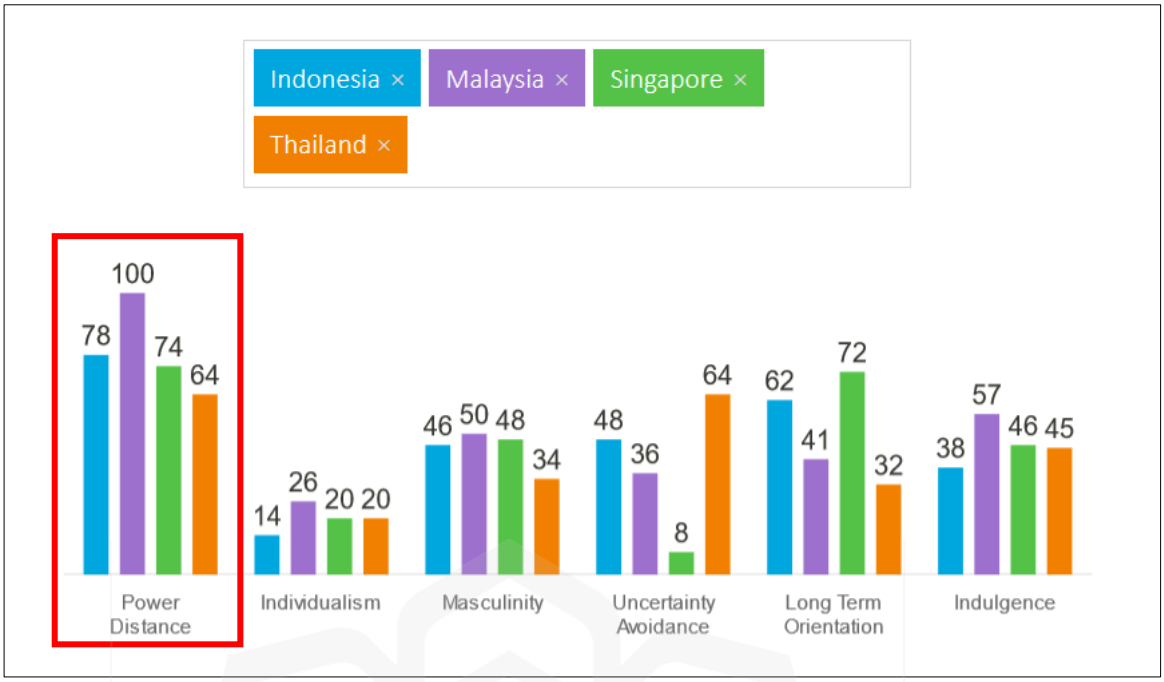


Figure 5.2: Values of power distance between Malaysia and other ASEAN countries (source: Hofstede Insights (2022))

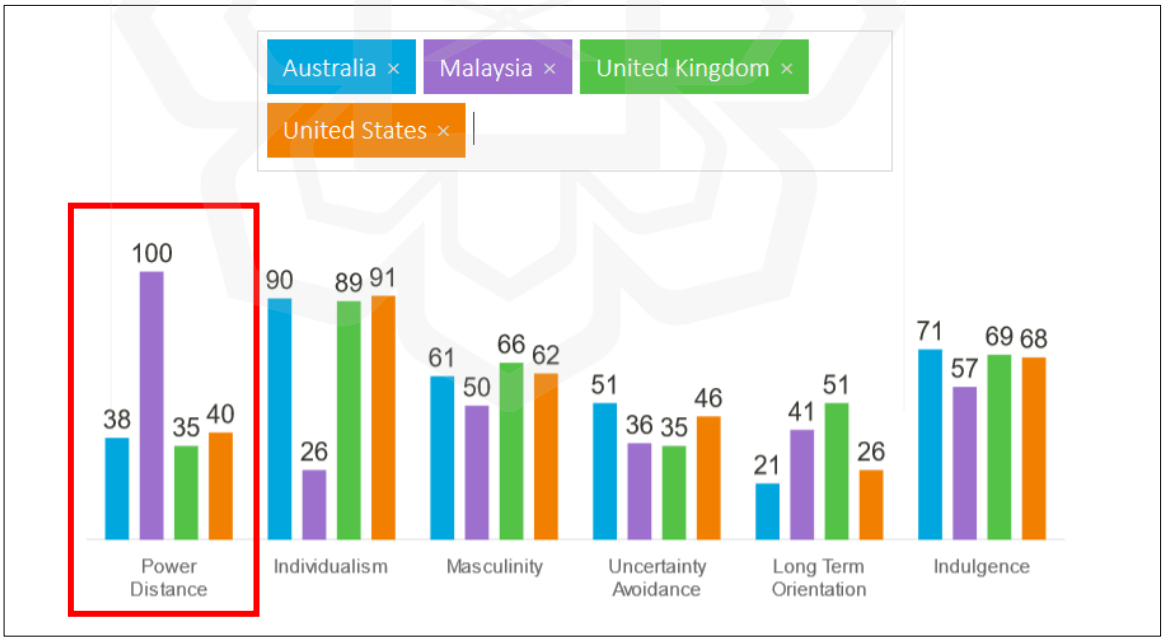


Figure 5.3: Values of power distance between Malaysia, Australia, United Kingdom and United States of America (source: Hofstede Insights (2022))

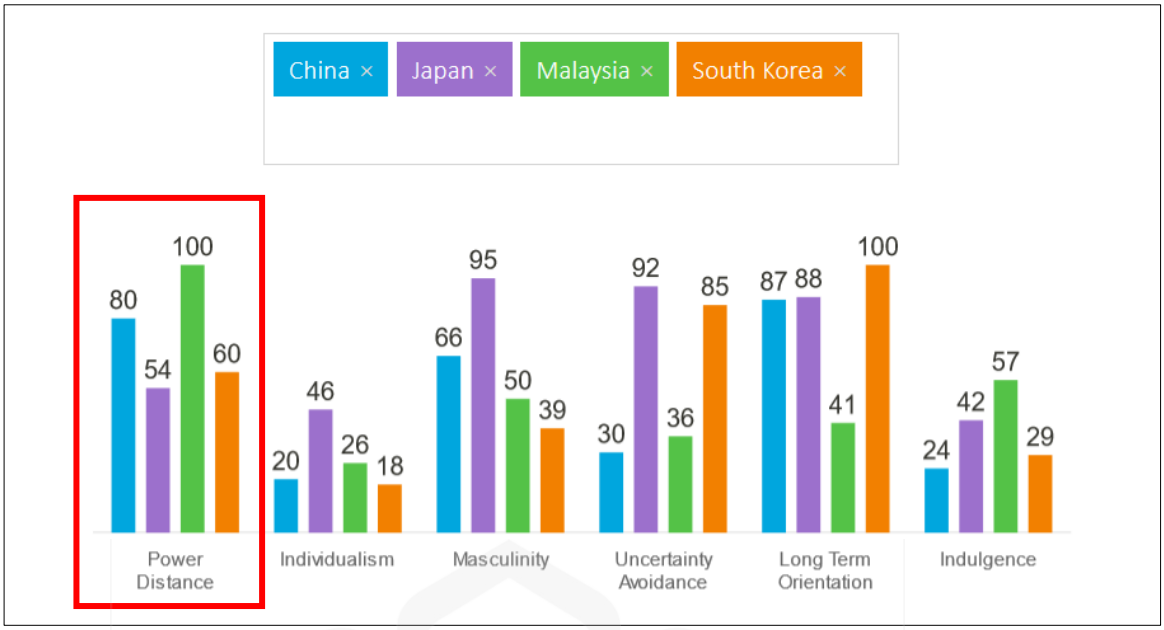


Figure 5.4: Values of power distance between Malaysia, China, Japan and South Korea (source: Hofstede Insights (2022))

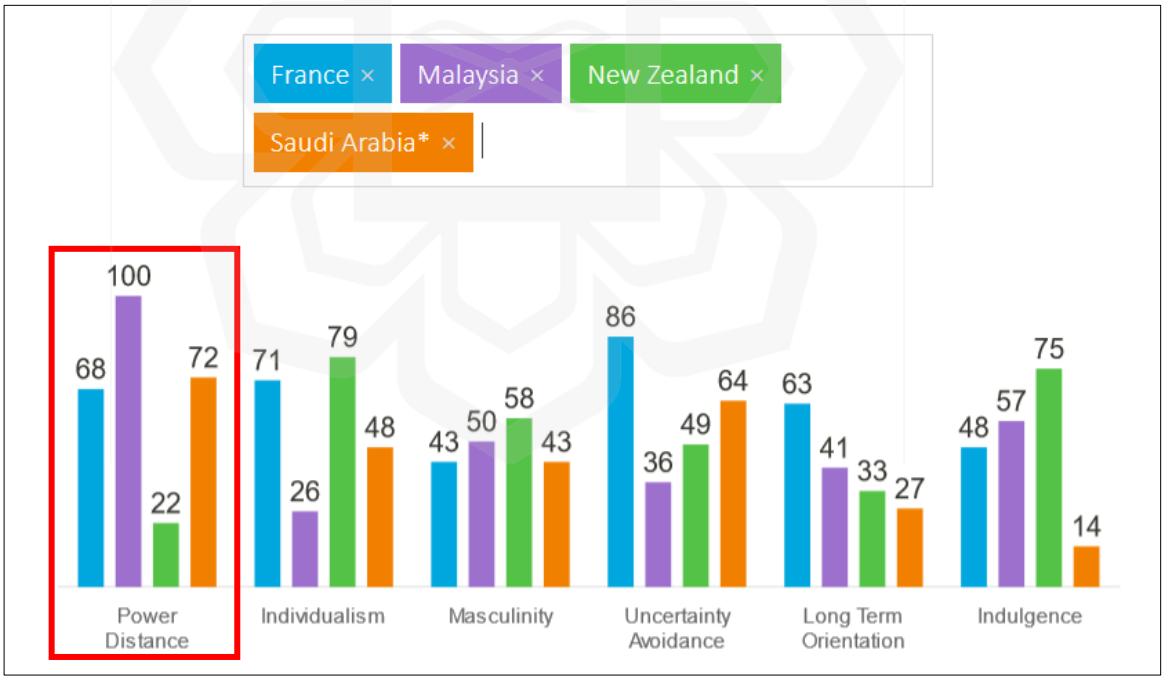


Figure 5.5: Values of power distance between Malaysia, France, New Zealand and Saudi Arabia (source: Hofstede Insights (2022))

Nevertheless, the findings presented in Section 4.3.1.1.1 demonstrate that the leadership style utilized by all four (4) businesses is a hybrid of Democratic (both ways) and Laissez-faire (bottom-up) approaches. Despite the fact that the power distance in Malaysia is very high and should result in an Authoritarian style, the researcher believes that the Authoritarian style has been moderated and becomes hybrid (Democratic and Laissez-faire) because top management and CIO rely on IT Division (Information Security Team) due to inadequate knowledge in information security matters (Laissez-faire). As previously stated in the findings section, because three (3) of the four (4) CIOs interviewed lack a background in information security education or at least formal education in the field of information technology, reliance on the division in providing directions and implementing information security activities is very high (Democratic). However, everything must be reported to the top management.

Unless it is reformed, the structure of information security governance in the Malaysian public sector organisations will continue to be led by the CIO or top management with diverse educational backgrounds, based on the value of the Power Distance owned by Malaysia.

5.6 CHAPTER SUMMARY

This chapter discussed the findings of the study based on themes and sub-themes elaborated in Chapter Four. The discussion incorporates and compares the findings drawn from the field investigation with the past literature. It started with a discussion on Information Security Governance Approach (derived from Theme 1) (Section 5.2), followed by Factors Influencing Top Management Engagement in Information Security (derived from Theme 2) (Section 5.3), and finally on the Information Security Governance Issues (derived from Theme 3) (Section 5.4). This final part of this chapter discusses the emerging findings (Section 5.5) before this study can be concluded in the next section.

CHAPTER SIX

CONCLUSION

6.1 OVERVIEW

The determinants impacting top management engagement in Malaysian public sector organisations are investigated in this thesis. It emphasises the problem's context, leading to the problem statement, research questions, and objectives (Chapter One). Relevant literature, concepts, and models linked to the investigated study are evaluated, as well as an overview of Malaysian information security implementation and its significant initiatives (Part I, Chapter Two). In order to construct the initial research model for this study, the relevant theory is examined and adapted to become the baseline of the model framework. The plausible factors influencing top management involvement are then deduced from theories and previous works of literature (Part II, Chapter Two). The research methodology is described in detail, along with a list of proposed methods and instruments for addressing research objectives (Chapter Three). The following three (3) chapters report the field investigation work, which includes data analysis, conclusions, and discussion (Chapter Four, Five and Six).

This chapter concludes the study by addressing the study's outcomes that answer the research questions and fulfil the research objectives. Then, the revised research model is presented. This chapter also indicates the contribution and limitations of this study. The last section of the chapter ends with a discussion on future work coming from this research. This chapter is organised as in Figure 6.1.

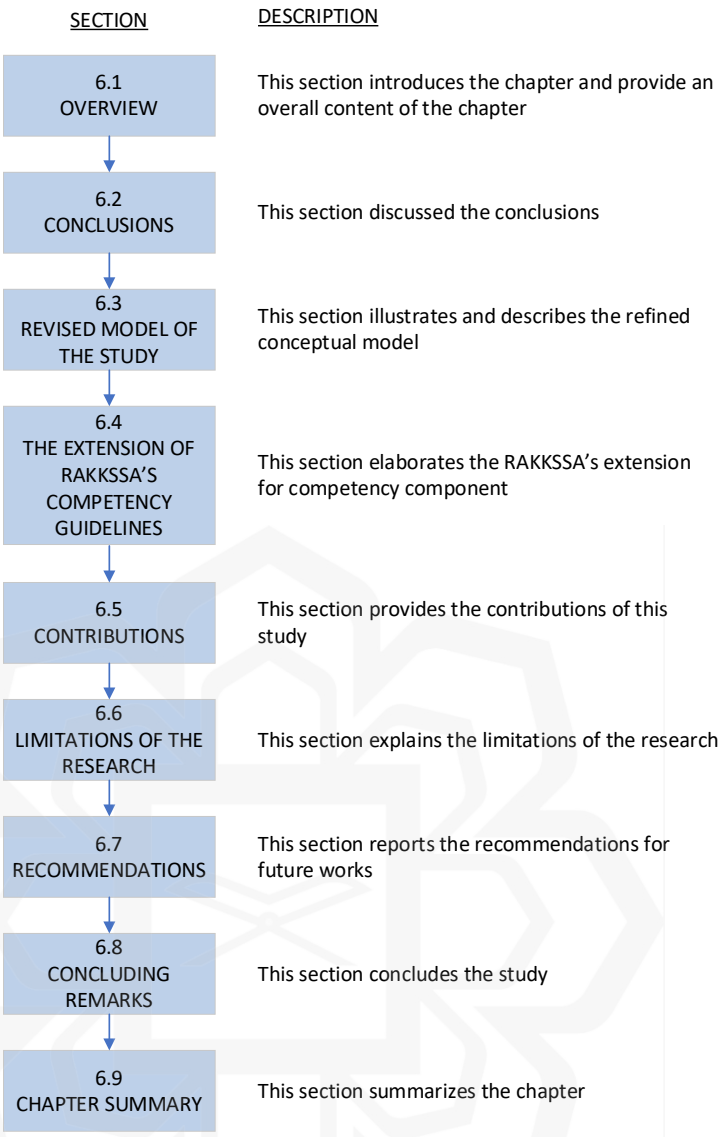


Figure 6.1: Organisation of Chapter Six

6.2 CONCLUSIONS

Results are summarised and discussed in light of the study's three (3) stated research objectives and the questions posed in the introduction (Section 1.4 and 1.5). The first objective is to investigate the way top management in the Malaysian public sector governs information security initiatives in their organisations. Second, to determine the factors influencing top management engagement in information security initiatives throughout the organisation's governance process. The revised research model for the factors is also presented. Third, to learn more about the issues faced by top management

in leading information security initiatives in their organisations. When these three (3) goals are met, a thorough understanding of information security governance in Malaysian public sector organisations, including the factors that motivate top management engagement in information security, is achieved.

6.2.1 Information Security Governance Approach

The study's first question is, *'How does top management govern information security in organisations?'*. It is accomplished by comprehending the previous literature in Chapter 2, and this study adapted the cycle of Direct-Implement-Check from Von Solms & Von Solms (2009)'s formal structure of information security governance. This study mapped and structured the roles and responsibilities of top management in governing information security into a suitable information security governance approach. The approach was then reviewed, revised, and updated in light of the field investigation findings. It was also improved during the early stages of developing research instruments that included interview questions. Table 6.1 depicts the information security governance approach based on the findings of this study and the literature review.

Table 6.1: Information security governance approach based on the research findings and the literature review

Roles and Responsibilities of Top Management in ISG based on the Research Findings	**Roles and Responsibilities of Top Management in ISG based on the Literature Review**	
▪ Top management practices in governing information security o Compliance with the public sector's information security direction o Communication of information security awareness and initiative o Enforcement against information security misconduct	▪ Have a sound knowledge of information security ▪ Formulate information security policies and directions ▪ Ensure alignment between business objectives with IT and risk management ▪ Set priorities and ensure measurable improvements in information security ▪ Inculcate security culture by leading through example ▪ Constantly remind employees about the importance of complying with the information security policy and its the implication of not doing so	**DIRECT**
▪ Top management leadership style in governing information security o Laissez-Faire (bottom-up) o Authoritarian (top-down) o Democratic (both ways)	▪ Define and assign responsibilities to the management level	

Roles and Responsibilities of Top Management in ISG based on the Research Findings	Roles and Responsibilities of Top Management in ISG based on the Literature Review	
▪ Information security budget o The approved information security budget o Case-based budget approval	▪ Provide appropriate security investments and adequate resources for security programs	IMPLEMENT
▪ Platform to discuss information security o Top management meeting o Steering Committee for ICT and Security (JPICT) o Committee for ISMS	▪ Provide visible support and commitment ▪ Subscribe to security assurance from security audit	
▪ Employee competency development in information security o Training for information security employees o Information security awareness to all employees	▪ Provide resources for information security education, training, and awareness programs to employees	
▪ Monitoring of information security implementation o Presentation by the information security team in meeting/audit meeting o Establishment of committee o Information security reports or meeting minutes submitted to top management	▪ Monitor and measure information security programs and their implementation	CHECK

According to Table 6.1, the study findings conclude that:

- The governance structure of each ministry and government agency is pretty identical. Each case study demonstrates that a consistent administrative pattern is probably the result of the impact of a central agency, such as MAMPU, which functions as a referral agency for ICT.
- The information security strategic plan in the Malaysian public sector is relatively well-organised, and regulations protecting sensitive materials are in place. Top management also plays a role in communicating information security awareness to employees. There are efforts made by the government through central agencies like MAMPU and NACSA to develop a cyber security strategy and framework to deal with the information leakage issues and to preserve the CIA of government information
- Top management, through the information security team, ensures that the organisation's information security initiatives are always in compliance with the public sector's security direction by referring to the Central Agency, which is MAMPU and NACSA. Top management uses opportunities such as meetings, monthly gatherings and events to remind employees of the importance of preserving organisational information assets. There is also an enforcement of any security misconduct that leads to the organisation's confidential information being disclosed to individuals or other unauthorised parties.
- The leadership style practised in all four (4) organisations could be described as a *hybrid of Democratic (both ways) and Laissez-faire (bottom-up).* In all organisations, the IT Division is given the autonomy to determine the implementation of information security within the organisation (Laissez-faire), but they are required to report all information related to the implementation to the top management. Top management's involvement entails providing feedback and endorsement on the IT Division's information security policy and approving the proposed information security activities (Democratic).
- Two (2) channels are used to distribute budgets to all divisions. The first method is through a financial allocation that has been given to each division or department. The budget for the information security project is allocated to the IT Division and then divided according to the project's priority under each unit

within the division. Secondly, the distribution of financial resources depends on the project's significance. This allocation considers the prompt execution of the ad hoc project, and the top management makes this decision.

- Three (3) main platforms have been employed that address all aspects of information security: The top Management Meeting, the Steering Committee for ICT and Security (JPICT), and the Committee for ISMS.
- Every employee in the public sector is required to have at least seven (7) days of training. This training includes not only training specific to the job at hand but also in any other form, as well as speeches, seminars, and other similar events like technology update sessions. In terms of communicating information security awareness to all employees, the information security team is in charge of implementing information security programs and activities, including briefing sessions.
- The information security unit carries out the implementation of information security. Top management monitors all actions and tasks through the presentation of information in meetings or audit meetings, the establishment of committees, and the reading of reports or meeting minutes that are routinely submitted, as well as when information security incidents occur.

6.2.2 Factors Influencing Top Management Engagement

The second research question is, '*What are the factors influencing top management engagement in organisations?'*. Thus, an initial research model was developed to address this research question after considering various models from earlier research. The foundation of this study's initial research model comprises three (3) elements; the Multiple Perspective Concept as the framework and the forces from the Neo-Institutional Theory (NIT). Other plausible factors which influence top management engagement in information security were derived from past literature.

Part II of Chapter Two mentioned that several external factors, such as the Coercive and Mimetic factors stated in the Neo-Institutional Theory and the Regulatory Forces from the prior research, are believed to influence the engagement of top

management in information security. However, these external factors do not align with the Multiple Perspectives Concept, which describes a scenario from three (3) perspectives: Technical (T), Organisational (O), and Personal (P) (P). A new stance called “External (E)” must be introduced to incorporate the external determinants into the Multiple Perspectives framework.

However, after conducting field investigation, the study concludes that there are no reasonable technical determinants, as shown in Table 6.2. Therefore, instead of integrating External (E) and Technical (T) perspectives, this study suggests replacing Technical (T) perspectives with External (E), and this substitution is justifiable based on this study’s findings.

Table 6.2: The influencing factors of top management engagement in information security based on the research findings and the literature review

Factor	**After field investigation**	**From previous literature**
External	(i) Regulatory forces (ii) Imitating good practice (iii) Changes in security risk exposure (iv) Audit compliance	(i) Regulatory forces (ii) Imitating good practice
Organisational	(i) Information security committee structure (ii) Culture (iii) Information security risk awareness (iv) Reputation	(i) Organisation’s condition (ii) Organisation’s size (iii) Work patterns and practices (iv) Reputation
Personal	(i) Formal education (ii) On-the-job exposure (iii) Informal education	(i) Age (ii) Formal education (iii) On-the-job exposure (iv) Informal education

Factor	After field investigation	From previous literature
		(v) Tenure in company

According to Table 6.1, the study results show that:

- The factors influencing top management engagement in information security are divided into three (3) categories: External, Organisational, and Personal. These criteria are categorised according to the Multiple Perspectives Concept, which includes Technical (T, but substitute to External (E)), Organisational (O), and Personal (P).
- Regulatory Forces (External Factor) is the sub-factor that received the most quotations from the participants across the cases, as shown in Table 4.8 (Chapter Four). 22 out of 27 participants agreed that top management would engage more in information security initiatives when there are directives from the external authority, i.e. Cabinet, instructions, circulars, and regulations from the Chief Government Security Office (CGSO), MAMPU and other higher authoritative bodies.
- Similarly, Informal Education (Personal Factor) is the most frequently mentioned sub-factor, cited by 22 participants, the same number of participants who discussed the Regulatory Forces factor. Top management with an adequate understanding of information security and who educated themselves through self-study and reading tend to engage more in information security efforts.
- On-The-Job Exposure (Personal Factor) is ranked the third most quoted factor by 18 participants. It is possible that top management does not have a formal educational background in information security because of the nature of the work they do; nonetheless, in order to fulfil their job requirements, they are still expected to be educated about and involved in information security. Because of this, it has an impact on the way they participate in information security.

6.2.3 Issues in Information Security Governance

The third research question is, *"What are the issues faced by the top management in governing information security in their organisation?"*. In addition to identifying the factors that influence the engagement of top management in information security, the case studies also provided insight into the issues surrounding information security governance in Malaysian public sector organisations. It is accomplished through knowledge of past literature on security governance issues (Chapter Two), analysis of case studies (Chapter Four) and discussion of the topic (Chapter Five).

These issues include the constraints top management faces in handling information security in their organisation, constraints in managing financial and labour resources, and constraints in cultivating information security culture, including employee acceptance of such culture, as depicted in Table 6.3.

Table 6.3: Issues in information security governance based on the research findings and the literature review

Issues retrieved from research findings	**Issues from the literature review**
▪ Top management constraint o Limited bandwidth due to hectic schedule and various meeting agenda o Inadequate knowledge and experience in information security o Reactive in handling information security issues o Information security is not an integral part of the organisation's business	▪ Top management always sees information security as an operational and technical issue ▪ The responsibility to manage the protection of information is often relegated to the ICT department or the small security team in the organisation. ▪ Top management may not have sufficient ICT knowledge and

Issues retrieved from research findings	Issues from the literature review
○ Generation gap of top management ▪ Resource constraint ○ Insufficient budget allocation ○ Insufficient human capital ▪ Challenges in employee acceptance of information security ○ Difficult to control staff ○ Employee lack of information security awareness ▪ Organisation's culture ○ Focus only on passing audit compliance ○ The misconception of information security and ownership ○ Difficult to change job routines	expertise to give security direction and IT-related strategies ▪ Top management does not understand their roles and responsibilities in ISG and ITG, which leads to minimal participation in information security initiatives in their organisation ▪ Difficult for top management to join the information security committee, even though they are expected to play a key role ▪ IT and security matters are also not included in the agenda of top management meetings ▪ Top management also has no time to involve in security as they have many things on their plate

According to Table 6.3, the study's findings indicate:

- The CIO, who represents the organisation's top management overseeing information security activities, has a demanding workload. This is because the CIO has a primary job as a deputy secretary-general for the ministry, depending on the ministry's core business, which often includes policy, administration, and development of the organisation. Moreover, the CIO role is an integral part of the position.

- The majority of CIOs do not have an IT background. Thus, the CIO relies heavily on the IT Division, particularly the information security team, when making decisions about information security.
- In the Malaysian public sector, it is typical for organisations to take a reactive strategy to handle issues and incidents involving information security.
- Information security initiatives receive the least attention from the organisation's top management since, in their view, information security is more of a support role than a crucial element of the organisation's operations.
- Participants believe that older generations of top management have trouble understanding information security and technology due partly to the generation gap.
- In terms of financial constraints, this is something that every public sector organisation expects. Top management must exercise caution when spending money and selecting and prioritising projects that appear to be more critical. Information security efforts must compete for funding with other projects.
- Top management faces significant hurdles in raising awareness and controlling employees' use of social media to share the organisation's confidential information, whether intended or unintentional.
- The organisations already have a culture where the information security audit focuses more on acquiring certification than nurturing information security itself.
- Employees also find it tough to adapt work patterns to comply with the information security policy.
- Perceptions that the task of protecting confidential information is the sole responsibility of the IT Division also become an issue that is difficult to change.

6.3 REVISED MODEL OF THE STUDY

In Chapter Two, this study represented the initial research model of the factors influencing top management engagement in information security, focusing on four (4) organisations in the Malaysian public sector. The initial research model resulted from a

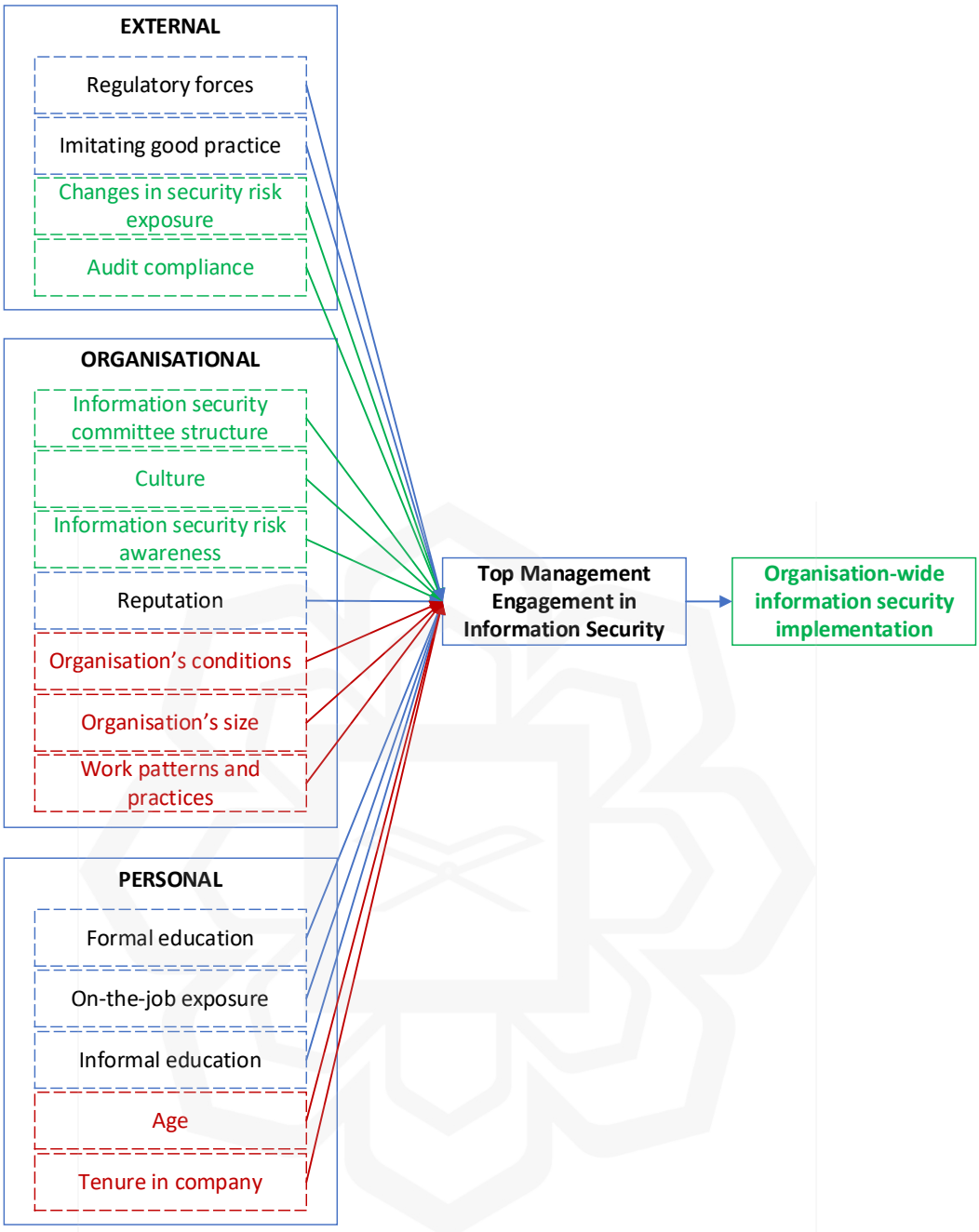
comprehensive analysis of the past literature, including the theories, concepts and definitions of information security and governance. The initial model has provided a solid foundation for further understanding the determinants that affect the engagement of top management in information security initiatives within their organisations. After the field investigation done in all four (4) case studies, the research model has been reviewed and refined to accommodate the findings. The *qualitatively validated model* produces a revised model that accommodates all modifications. Figure 6.2 shows the difference between the initial research model and the revised model of this study.

Based on Figure 6.2, after conducting multiple-case studies on four (4) public sector organisations, numerous modifications were made to the initial research model as illustrated in Chapter Two (See Section 2.12.3). The modification of the initial research model based on findings from the multiple-case study is part of the process of producing a qualitatively validated model (revised model) from the initial model. Five (5) new factors were added to the revised model, while five (5) factors were eliminated.

Changes in Security Risk Exposure [ranked 8] and Audit Compliance [ranked 6] are among the five (5) factors that fall under External Factor. Under Organisational Factor, the remaining three (3) factors are Information Security Committee Structure [Ranked 7], Culture [Ranked 11], and Information Security Risk Awareness [Ranked 4]. Participants agreed that these five (5) factors significantly impact top management engagement in information security initiatives. Table 4.8 displays the proportion of participants who concur with these factors. Based on the findings provided by the participants, the researcher determined that these new factors were significant; consequently, they were incorporated into the revised model for this study.

On the other hand, the revised model eliminates five (5) factors: Organisational Conditions, Organisation's Size, and Work Patterns and Practises. These three factors fall under the Organisational Factor. Age and Tenure in the Company are the other two eliminated factors. All participants agree that the Organisation's Size, Age, and Tenure in the Company have no bearing on top management's engagement in information security. In contrast, the terms Organisational Conditions and Work Patterns and Practices are given a new phrase that provides a more accurate meaning and more

clearly reflects the participant's point of view. For example, Culture factors replace Organisational Conditions, and Information Security Committee Structure replaces Work Patterns and Practices. Figure 6.3 depicts, and the following paragraph describes, the establishment of the revised model linked to this study's primary issue.



*__Note(s)__:
Green color denotes the factor and element that were added to the revised model
Red color denotes the factor that were eliminated from the revised model
Black/Blue color denotes the consistent factor

Figure 6.2: The difference between the initial and the revised research model

According to the existing literature, numerous studies have found a *correlation* between *the involvement of top management* in information security and *the acceptance and implementation of information security throughout an organisation* (AlGhamdi et

al., 2020; Al-Izki & Weir, 2016; Alshaikh et al., 2022; Hu et al., 2007a; Kim & Kim, 2015). It is challenging to materialise organisation-wide information security implementation and activities without sufficient top management commitment and support (Kim & Kim, 2015). Again, the engagement of top management is crucial, especially when organisations attempt to implement reasonable security practices based on excellent security rules. With a top-down approach, where engagement of top management is strengthened, norms are established and followed uniformly. Employees were transformed into assets rather than threats (Alshaikh et al., 2022), thus inspiring them to do their duties (AlGhamdi et al., 2020; Al-Izki & Weir, 2016). Security procedures are being adopted as organisation-wide policies as opposed to just the policy of one department (Hu et al., 2007a). When this happens, information security initiatives can be easily implemented across the organisation.

Thus, based on the findings of these studies, it is evident that *the involvement of an organisation's top management is essential for a successful rollout of information security measures in the whole organisation*. Consequently, identifying the factors that influence the participation of top management in information security initiatives can alleviate the issue where the information is challenging to implement and appreciate across the entire organisation. This is the primary issue highlighted in Chapter One (see Section 1.3 - Statement of the Problem), which resulted in the three (3) problems listed in the section. Therefore, there is a correlation between the factors that influence top management engagement in information security and the implementation of security across an entire organisation. As depicted in Figure 6.3, the qualitatively validated model is therefore linked to the primary issue of this study.

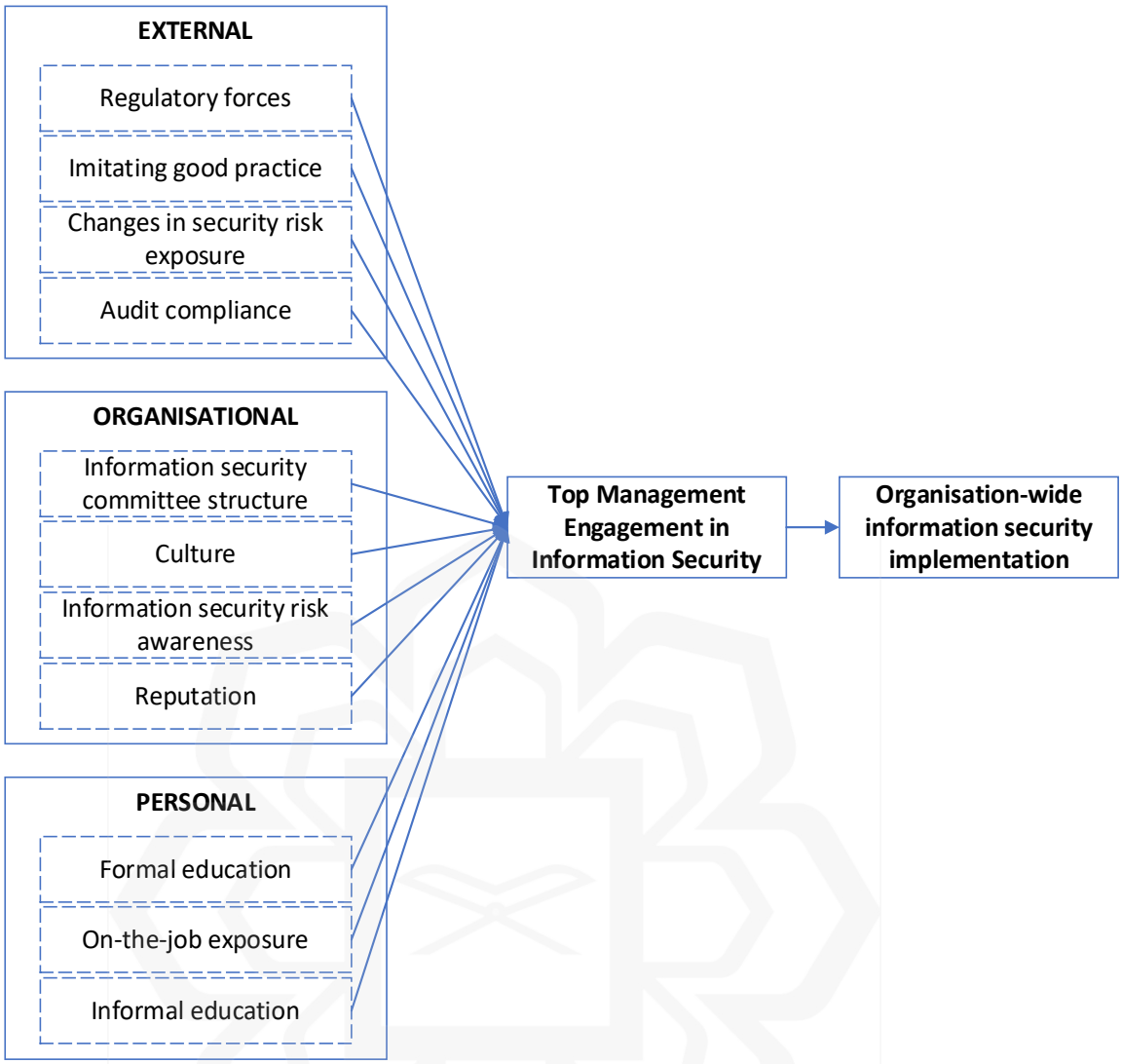


Figure 6.3: Revised model of the factors influencing top management engagement in information security

6.4 THE EXTENSION OF RAKKSSA'S COMPETENCY GUIDELINES

Past studies have concluded that information security governance must be handled at the highest levels of an organisation. In a similar vein, the researcher found that the top management, in this case referring to the CIO, is struggling to execute their roles and responsibilities in governing information security, leading to the emerging findings discussed in Chapter Four.

Nevertheless, the RAKKSSA's competency components do not mandate the required competency for top management. Top management needs specific skills to carry out their duties as decision-makers of information security initiatives within their organisations. If RAKKSSA does not provide a guideline for the competency required for top management, it will be challenging to put the governing structure in place. Information security practises are harder to implement and appreciate throughout the organisation, which is related to the issue and problems mentioned in the problem statement of this study.

Therefore, this study maps the top management's influencing factors on the engagement in information security and the roles and responsibilities of top management from prior literature to a new proposed extension of RAKKSSA focusing on top management competencies. This mapping led to the extension of RAKKSSA's competency guidelines for top management, as detailed in Appendix M. This extension ensures that the competency component of the customised information security policy developed by Malaysian ministries and public sector agencies will now include Top Management, End-users *(Pengguna)*, and Implementers *(Pelaksana)*.

6.5 CONTRIBUTIONS

This study adds to the body of knowledge in the field of information security governance. This section emphasises the study's theory, methodology, and practice contribution.

6.5.1 Theoretical Contribution

This study makes four (4) theoretical contributions: the introduction of a new perspective in MPC, the use of all three (3) categories in NIT, the development and establishment of a research model that provides new insights into the engagement factors of top management in information security, and the extension of the RAKKSA framework by addressing top management competency.

First, this study has introduced a new perspective known as "External (E)" within the framework of Multiple Perspectives. The study suggests integrating the External (E) view with the Technical (T) perspective in MPC. The rationale for this consolidation is supported by the findings of the study, which revealed a lack of significant factors within the Technical (T) lens. The modification made to the MPC expands the study's lens and viewpoint in examining the engagement issues by the top management.

Second, this study utilises all three (3) categories in Neo-Institutional Theory as determinants in modelling the factors influencing top management engagement in information security. Even though these factors may yield different outcomes depending on the time and case study settings, the study demonstrates how each factor emerged based on the interpretive explanation. The qualitative approach permits the comprehension and discovery of the organisation's context and how numerous factors and issues emerge during the investigation, thereby enhancing the significance of the findings. However, this scenario is challenging to measure quantitatively.

Third, the research model provides new insights in understanding top management engagement in information security in Malaysian government landscape. After the field investigation, the revised research model establishes a connection between the factors influencing the engagement of the public sector's top management in information security and the primary issue outlined in the problem statement (Chapter One), which becomes the motivation for this research. The research model highlights the numerous factors that trigger top management engagement in information security.

Fourth, as stated in Section 2.5.3.2, the RAKKSSA competency components only cover the necessary competency for End-User and Implementer but lack a requirement for the required competency for top management. Therefore, the case study findings related to the factors influencing top management engagement in information security are used to extend the RAKKSSA document, the highest level of MAMPU-developed cyber security framework. RAKKSSA is a fundamental guide and security component that Malaysian ministries and public sector agencies should follow to develop their information security policy and protect their information assets in

cyberspace. The findings discovered in this study's analysis are employed to create a guideline for top management competency, which was found to be lacking in the guideline. The competency criteria are essential for top management to understand their roles and responsibilities so that they would be able to play their part in the government's information security initiative. The extension of the cyber security framework, focusing on top management competency, is expected to produce more comprehensive, end-to-end guidelines to be utilised by all Malaysian public sectors in implementing information security efforts in their organisations.

6.5.2 Methodological Contribution

In this study, two (2) methodological contributions are recognised: the adaptation of Yin's multiple-case study method in Interpretive paradigm, and the use of Qualitative approach provide in depth data about the phenomenon under study.

The study employs Yin's multiple-case study method inside the interpretive paradigm. Despite Yin's inclination towards positivism in his approach to case study, the use of Yin's multiple-case study method inside the interpretive paradigm effectively captures the depth and complexity of the topic of information security governance and top management engagement. This study highlights the necessity of incorporating flexibility within research methodologies, enabling researchers to leverage the unique strengths offered by different paradigms.

The utilisation of qualitative research in this study enables the exploration and acquisition of extensive data pertaining to the issue being investigated. The study additionally demonstrates how inputs from many viewpoints can be employed to facilitate the collection and interpretation of data. The field investigation conducted in four (4) case studies includes interview sessions, which contribute to a comprehensive comprehension of the topic of top management engagement and give supporting evidence for the initial research model. The validation process for the initial research model involves modifying it based on evidence obtained from the application of various

case studies. Consequently, the initial research model underwent qualitative validation, leading to the development of the final model.

6.5.3 Practical Contribution

This study provides two (2) practical contributions: public and private sector organisations can use the research model to improve top management engagement by formulating personalized information security training. RAKKSSA's top management competency facilitates the Malaysia's central agency to produce a comprehensive cyber security framework.

Significant theoretical advancement has resulted from this work in the form of a useful revised model. This study expanded on current knowledge of information security governance as expressed in this study's literature by looking at the factors influencing top management engagement in security initiatives. The qualitatively validated model may be used by top management in the public and private sectors, IT staff, and the security community to investigate and evaluate the governance of information security initiatives at the organisation's highest levels. With this knowledge in hand, they will be better equipped to address concerns about information security acceptance and the support of top management. In addition, it will help with the skewed perspective on information security and attempts to minimise it. This will allow for better acceptance and implementation of the information security initiative, increasing its value to the business as a whole. The training and outreach team can use the study's findings to tailor SETA for employees at all levels of the organisation. Employees can relate information security to their daily work resulting from the SETA program's ability to reach everyone in the organisation.

The extension of top management competency in RAKKSSA (cyber security framework) aids the central agency in developing an up-to-date version of the framework. Since the current framework only focuses on the competency of the user and implementer, the extension and the guideline model allow public sector organisations to ensure that their cyber security policy and documents address the

competency of top management in governing information security within their organisations. Therefore, regardless of rank, position, or job function, all levels within the ministry understand the roles and responsibilities associated with each government-wide information security initiative. Information security is not solely the IT department's or end-users' responsibility; instead, it is an organisation-wide collaborative effort. Therefore, it should be treated with the same importance as other business concerns. It begins with the top management's commitment and involvement.

6.6 LIMITATIONS OF THE RESEARCH

Despite the fact that it contributes to both theory and practice, this study has a few drawbacks that need to be considered. Other researchers can consider them before carrying out an investigation of a similar nature. The following are the study's limitations:

- Although the researcher encountered a few obstacles in obtaining the cooperation of ministries and agencies involved in these case studies, it was challenging to schedule an appointment with top management due to their extremely tight work schedules. The study's findings would be strengthened if more perspectives from top management could be gathered. However, each case study contained at least one (1) representative of top management, of which three (3) were CIOs.
- When conducting research on information security with a particular emphasis on top management, gaining access to organisations and individuals willing to discuss sensitive information is one of the most challenging aspects of the research. Employees in the public sector who hold lower-level positions refuse to discuss their superiors and concerns regarding information security in their organisations, probably due to the power distance in Malaysia. Participants fear that telling the truth will jeopardise their jobs in the public sector. In addition, participants have the propensity to present a positive and secure image to the outside world, regardless of the existing circumstances within the organisation or the actual condition of information security.

6.7 RECOMMENDATIONS

Recommendations for this study are based on the study's findings and conclusions for this study. Several recommendations for future work can be carried out to extend this study. It is suggested that the organisations implement the revised model of the factors influencing top management engagement in information security and that the study be extended to include a more significant number of case studies, different levels of employees (especially top management), and different types of research. Alternatively, researchers have the option to focus their research efforts on a single case and delve into its intricacies.

Case studies for this research were carried out in different government organisations that have successfully implemented information security measures. Initiatives in the public sector aimed at improving information security are significantly influenced by the policies, guidelines, and standards formulated by central agencies such as MAMPU and NACSA. It is necessary to conduct additional case studies not only in the public sector but also in the private sector in order to comprehend and explore more additional factors that influence the involvement of top management in an organisation. Another aspect to be taken into consideration is the utilisation of a single case study approach, which would allow for a more comprehensive examination including a larger sample size of top-level management and staff. This will put the adaptability of the revised model to the test in various settings.

As stated in the preceding section, this research focuses on top management engagement in information security. This research should be expanded to include a broader range of correlations, such as how the factors influencing top management engagement affect their attitude and behaviour and vice versa. Revised models should also be used to delve deeper into other influencing elements, such as how top management engagement relates to the critical success factor of information security. Furthermore, more factors affecting top management engagement in information security can be discovered in the same or different context. As a result, additional elements can be explored and found, and similarities and differences can be compared and contrasted.

Future research should ideally be conducted using other qualitative methods, such as Action Research, Ethnographic Studies, and Grounded Theory. Utilizing various qualitative research methods will allow for a deeper understanding of the top management's involvement in information security within the organisation. Research utilising the revised model generated by this study can also be continued using a quantitative strategy, such as questionnaires, or a mixed method to yield broader findings. This methodology can encompass a larger sample size and permit generalisations about the phenomenon of top management participation in the information security initiative. Obviously, if different methods were employed in the context of this study, more emerging and exciting findings would be generated and could be learned to contribute to the body of knowledge.

6.8 CONCLUDING REMARKS

This chapter wraps up the entire thesis by answering all the research questions and accomplishing the research objectives outlined in the introduction. The study's theoretical contribution and methodological and practical approach are then discussed. The study's limitations are outlined as well. Finally, it recommends how this research's theoretical underpinnings, practical applications, and potential outcomes can be developed further.

Understanding research problems and finding solutions to research questions have been made possible by the interpretive paradigm chosen to carry out this study. It is common for researchers to stray from their initial plan while digging into a problem. Throughout the course of the study, even the planning process underwent several iterations. However, this is a normal occurrence when conducting explorations of this interpretation research. Despite the revisions, this final section of the study has proven that all goals can be achieved.

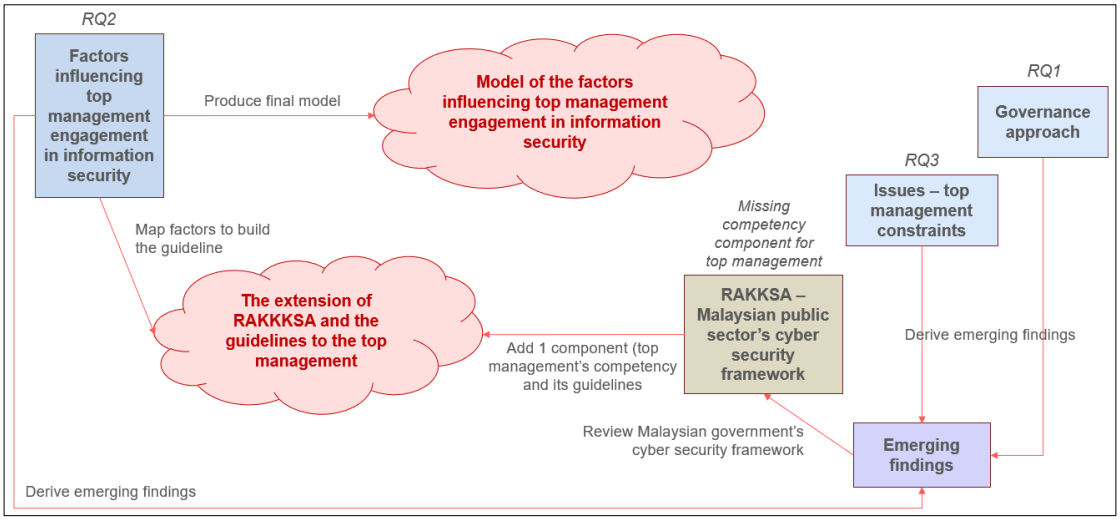


Figure 6.4: The overall research contribution

Figure 6.4 illustrates the overall research contribution. The study's findings offer a completely revised model of the factors that influence top management's engagement in information security. The initial research model serves as a foundation for research (data collection and analysis) and explains the consensus of views on information security governance held by four (4) case studies of Malaysian public sector organisations. Applying research models to case studies enables the identification of information security approaches, the influencing factors, and the revolving issues around information security governance. When comparing what the researchers discover in the literature, which is mainly based on the results of research conducted in other countries and may also differ in other organisations, these case studies allow for the identification of criteria relevant to the settings of organisations in Malaysia. The field investigation of multiple case studies provided evidence for the initial research model. Modifications to the initial research model become the process of validating the model, thus resulting in a qualitatively validated model. The study's linkages and contributions are summarised in Table 6.4.

Table 6.4: The study's linkages and contributions

ISSUE	PROBLEM STATEMENT	RESEARCH OBJECTIVE (RO)	RESEARCH QUESTION (RQ)	RESEARCH OUTCOME	RESEARCH CONTRIBUTION
Information security practices are challenging to implement and appreciate throughout the organisation		**Primary RO:** To understand how can top management engagement in information security be improved in Malaysian public sector organisations	**Primary RQ:** How can top management engagement in information security be improved in Malaysian public sector organisations?		
	Sub-problem 1: Information security matters delegated to the information security team *(How is the current implementation?)*	**RO1:** To investigate how top management drives information security initiatives within Malaysian public sector organisations.	**RQ1:** How does top management govern information security in organisations?	**Information security governance approach** *(para 5.2 and 6.2.1)*	1) The model of the factors influencing top management engagement in information security

ISSUE	PROBLEM STATEMENT	RESEARCH OBJECTIVE (RO)	RESEARCH QUESTION (RQ)	RESEARCH OUTCOME	RESEARCH CONTRIBUTION
	Sub-problem 2: Engagement from the top management is low *(What are the factors affecting their engagement?)*	**RO2:** To determine the factors influencing top management engagement in information security governance **RO2.1:** To identify the determinants that influence top management engagement in information security **RO2.2:** To develop a research model based on the factors identified in RO2.1	**RQ2:** What are the factors influencing top management engagement in organisations?	❑ External ▪ Regulatory forces ▪ Imitating good practice ▪ Changes in security risk exposure ▪ Audit compliance ❑ Organisational ▪ Information security committee structure ▪ Culture ❑ Personal ▪ Formal education ▪ On-the-job exposure ▪ Informal education *(para 5.3 and 6.2.2)*	2) The extension of RAKKSSA's competency component and guidelines for top management *(the highest level of Malaysian public sector's cyber security framework)*

ISSUE	PROBLEM STATEMENT	RESEARCH OBJECTIVE (RO)	RESEARCH QUESTION (RQ)	RESEARCH OUTCOME	RESEARCH CONTRIBUTION
		RO2.3: To establish an extension of Malaysia's Cyber Security Framework (RAKKSSA) document and its accompanying guidelines based on the engagement factors		▪ Information security risk awareness ▪ Reputation	
	Sub-problem 3: Information security initiatives are treated as a one-off project rather than a continual process *(What are the issues revolved around*	**RO3:** To explore the issues related to top management governing information security initiatives in their organisations	**RQ3:** What are the issues faced by the top management in governing information security in their organisation?	**Issues revolving around information security governance** *(para 5.4 and 6.2.3)* **Emerging findings (from RQ1, RQ2, RQ3)** *(para 5.5)*	

ISSUE	PROBLEM STATEMENT	RESEARCH OBJECTIVE (RO)	RESEARCH QUESTION (RQ)	RESEARCH OUTCOME	RESEARCH CONTRIBUTION
	information security governance?)				

As mentioned before, the information security implementation in Malaysian public sector organisations should be accepted, valued and implemented by all levels of the organisation. Good policies, guidelines, and standards formulated by central agencies such as MAMPU and NACSA should be an organisation-wide collaborative effort rather than a responsibility of the IT Division within the organisation. It would be unfortunate if the Malaysian government had comprehensive information security policies, guidelines, and standards in place but ultimately failed to put them into practice. In this regard, top management plays an essential part in ensuring that everyone in the organisation, regardless of rank, position, or job function, adheres to the organisation-wide information security policies and responsibilities. Everybody should be aware and practice their roles and responsibilities and treat information security matters equally to other business concerns. Therefore, this study proposes extending the RAKKSSA's competency guidelines for top management. The guideline enables ministries and agencies in the Malaysian public sector to develop end-to-end information security policies and guidelines that serve the implementer and end-user and the most critical group in information security governance, the top management. Furthermore, the inclusion of top management responsibilities should encompass all government official documents related to cybersecurity governance, risk and compliance.

Information security professionals and policymakers alike can benefit from keeping an eye on this study's findings as they work to strengthen information security programs across the country. Relevant stakeholders, equipped with knowledge of the findings from different points of view, should be able to propose ways to improve the present implementation of information security within their organisations and throughout Malaysia.

6.9 CHAPTER SUMMARY

This chapter concluded the study by discussing the achievements in meeting the three research objectives and questions (Section 6.2). The revised model of the factors influencing top management engagement in information security is illustrated and

discussed (Section 6.3), followed by the extension of RAKKSSA's competency guidelines for top management (Section 6.4), contributions of this study (Section 6.5), its limitations (Section 6.6), and its recommendations (Section 6.7). This chapter's final section explains the study's concluding remarks (Section 6.8).

REFERENCES

Abdul Molok, N. N., Chang, S., & Ahmad, A. (2013). *Disclosure of Organizational Information on Social Media: Perspectives from Security Managers*. 1–12. http://jbis.cafe24.com/data/pacis2013_submission_538.pdf

Abu-Musa, A. (2010). Information Security Governance in Saudi Organizations: An Empirical Study. *Information Management & Computer Security*, *18*(4), 226–276. https://doi.org/10.1108/09685221011079180

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, *72*, 361–373. https://doi.org/10.1016/j.procs.2015.12.151

Ahmad, A., Ruighaver, A., & Teo, W. (2005). An Information-Centric Approach to Data Security in Organizations. *TENCON 2005 - 2005 IEEE Region 10 Conference*, 1–5. https://doi.org/10.1109/TENCON.2005.301322

Albrechtsen, E. (2007). A Qualitative Study of Users' View on Information Security. *Computers & Security*, *26*(4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information Security Governance Challenges and Critical Success Factors: Systematic Review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Al-Izki, F., & Weir, G. R. S. (2016). Management Attitudes toward Information Security in Omani Public Sector Organisations. *2016 Cybersecurity and Cyberforensics Conference (CCC)*, 107–112. https://doi.org/10.1109/CCC.2016.28

Allen, J. (2005). *Governing for Enterprise Security* (CMU/SEI-2005-TN-023; p. 82). Carnegie Mellon University.

Allen, J. H., & Westby, J. R. (2007). Characteristics of Effective Security Governance. *EDPACS*, *35*(5), 1–17. https://doi.org/10.1080/07366980701394229

Alshaikh, M., Chang, S., Ahmad, A., Maynard, S. B., & Alammary, A. (2022). Embedding Information Security Management in Organisations: Improving Participation and Engagement Through Intra-Organisational Liaison. *Security Journal*. https://doi.org/10.1057/s41284-022-00352-3

Armstrong, C. P., & Sambamurthy, V. (1999). Information Technology Assimilation in Firms: The Influence of Senior Leadership and IT Infrastructures. *Information Systems Research*, *10*(4), 304–327. https://doi.org/10.1287/isre.10.4.304

Avison, D. E., Lau, F., Myers, M. D., & Nielsen, P. A. (1999). Action Research. *Communications of the ACM*, *42*(1), 94–97. https://doi.org/10.1145/291469.291479

Babbie, E. R. (2016). *The Practice of Social Research* (Fourteenth edition). Cengage Learning.

Bacharach, S. B. (1989). Organizational Theories: Some Criteria for Evaluation. *The Academy of Management Review*, *14*(4), 496. https://doi.org/10.2307/258555

Bahagian Kabinet, Prime Minister's Department. (2022, April 11). *Prime Minister's Department*. https://www.kabinet.gov.my/bkpp/index.php/anggota-pentadbiran/menteri

Baptiste, I. (2001). *Qualitative Data Analysis: Common Phases, Strategic Differences*. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research. http://nbn-resolving.de/urn:nbn:de:0114-fqs0103226

Barki, H., & Hartwick, J. (1989). Rethinking the Concept of User Involvement. *MIS Quarterly*, *13*(1), 53. https://doi.org/10.2307/248700

Barton, K. A. (2014). *Information System Security Commitment: A Study of External Influences of Senior Management.pdf*. Nova Southeastern University.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly/September 1987*, 369–386.

Benton, T., & Craib, I. (2011). *Philosophy of Social Science: The Philosophical Foundations of Social Thought* (2nd ed., 10th anniversary ed). Palgrave Macmillan.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. https://open.umn.edu/opentextbooks/BookDetail.aspx?bookId=79

Bjorck, F. (2004). Institutional Theory: A New Perspective for Research Into IS/IT Security in Organisations. *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of The*, 5 pp. https://doi.org/10.1109/HICSS.2004.1265444

Boitan, I. A. (2019). *Cyber Security Challenges through the Lens of Financial Industry*.

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bruin, R. D., & Von Solms, S. (2016). *Cybersecurity Governance: How Can We Measure It?* 1–9.

Budzak, D. (2016). Information Security—The People Issue. *Business Information Review*, *33*(2), 85–89. https://doi.org/10.1177/0266382116650792

Burrell, G., & Morgan, G. (2011). *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life* (Reprinted). Ashgate.

Cambridge Dictionary. (n.d.). *ENGAGEMENT | meaning in the Cambridge English Dictionary*. Retrieved 25 July 2022, from https://dictionary.cambridge.org/dictionary/english/engagement

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional Pressures in Security Management: Direct and Indirect Influences On Organizational Investment in Information Security Control Resources. *Information & Management*, *52*(4), 385–400. https://doi.org/10.1016/j.im.2014.12.004

Chang, S. E., & Ho, C. B. (2006a). Organizational Factors to the Effectiveness of Implementing Information Security Management. *Industrial Management & Data Systems*, *106*(3), 345–361.

Chang, S. E., & Ho, C. B. (2006b). Organizational Factors to The Effectiveness of Implementing Information Security Management. *Industrial Management & Data Systems*, *106*(3), 345–361. https://doi.org/10.1108/02635570610653498

Charmaz, K. (2006). *Constructing Grounded Theory*. Sage Publications.

CNII Portal. (n.d.). Retrieved 11 August 2017, from http://cnii.cybersecurity.my/main/ncsp/index.html

Corbin, J., & Strauss, A. (1990). *Grounded Theory Research: Procedures, Canons, and Evaluative Criteria*. *13*(1), 19.

Corsten, H. (1987). Technology Transfer from Universities To Small And Medium-Sized Enterprises – An Empirical Survey From The Standpoint Of Such Enterprises. *Technovation*, *6*(1), 57–68. https://doi.org/10.1016/0166-4972(87)90039-3

Craig, E. (1998). Routledge Encyclopedia of Philosophy. In *Routledge Encyclopedia of Philosophy*. Routledge.

Cresswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (4th ed). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th Edition). SAGE Publications, Inc.

Crotty, M. (1998). *The Foundations of Social Research: Meaning and Perspective in the Research Process* (1st ed.). SAGE Publications, Inc. https://doi.org/10.4324/9781003115700

CyberSecurity Malaysia. (2023). *MyCERT : Incident Statistics—Reported Incidents based on General Incident Classification Statistics 2023*. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=9a7531ad-6d35-4d95-bb13-e6f356cc2286

Denzin, N. K., & Lincoln, Y. S. (2005). *The SAGE Handbook of Qualitative Research* (3rd Edition). SAGE Publications, Inc.

Denzin, N. K., & Lincoln, Y. S. (2011). Introduction: The Discipline and Practices of Qualitative Research. In *The SAGE Handbook of Qualitative Research*. SAGE Publications, Inc.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited Institutional Isomorphism and Collective Rationality in Organizational Fields. In *Advances in Strategic Management* (Vol. 17, pp. 143–166). Emerald (MCB UP). https://doi.org/10.1016/S0742-3322(00)17011-1

DiMaggio, P. J., & Powell, W. W. (2000). The Iron Cage Revisited—Institutional Isomorphism and Collective Rationality in Organizational Fields. In *Advances in Strategic Management* (Vol. 17, pp. 143–166). Emerald (MCB UP). https://doi.org/10.1016/S0742-3322(00)17011-1

Djamba, Y. K., & Neuman, W. L. (2002). Social Research Methods: Qualitative and Quantitative Approaches. *Teaching Sociology*, *30*(3), 380. https://doi.org/10.2307/3211488

Doherty, N. F., & Fulford, H. (2006). Aligning The Information Security Policy with The Strategic Information Systems Plan. *Computers & Security*, *25*(1), 55–63. https://doi.org/10.1016/j.cose.2005.09.009

Dutta, A., & McCrohan, K. (2002). *Management's Role in Information Security in a Cyber Economy.pdf*. *45*(1). https://doi.org/10.2307/41166154

Dworkin, S. L. (2012). Sample Size Policy for Qualitative Studies Using In-Depth Interviews. *Archives of Sexual Behavior*, *41*(6), 1319–1320. https://doi.org/10.1007/s10508-012-0016-6

Ernst & Young. (n.d.). *Cybersecurity in TMT*. Retrieved 21 June 2022, from https://www.ey.com/en_gl/tmt/cybersecurity

Ernst & Young. (2016). *Final Report—Global Information Security Survey 2016*. http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016

Ernst & Young. (2023a). *How to balance opportunity and risk in adopting disruptive technologies*. https://www.ey.com/en_my/forensic-integrity-services/how-to-balance-opportunity-and-risk-in-adopting-disruptive-technologies

Ernst & Young. (2023b, October 2). *Cyber leaders' confidence in their organization's defenses plummets, but costs mount*. https://www.ey.com/en_gl/news/2023/10/cyber-leaders-confidence-in-their-organizations-defenses-plummets-but-costs-mount

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Gantz, S. D., & Philpott, D. R. (2013). *Chapter 13—Risk Management*. https://www.sciencedirect.com/topics/computer-science/security-risk-management

Gray, D. E. (2004). *Doing Research in the Real World*. Sage Publications.

Gregor. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611. https://doi.org/10.2307/25148742

Guba, E. G., & Lincoln, Y. S. (1994). *Handbook of Qualitative Research—Competing Paradigms in Qualitative Research*. SAGE Publications, Inc.

Guba, E. G., & Lincoln, Y. S. (2005). Paradigmatic Controversies, Contradictions, and Emerging Confluence. In *The Sage Handbook of Qualitative Research* (3rd Edition). SAGE Publications, Inc.

Gummesson, E. (2000). Qualitative Research Methods in Management Research. In *Journal of The Operational Research Society—J OPER RES SOC* (Vol. 44).

Guo, K. H. (2013). Revisiting the Human Factor in Organizational Information Security Management. *Isaca Journal*, *6*, 5.

Gupta, A., & Hammond, R. (2005). Information Systems Security Issues and Decisions for Small Businesses: An Empirical Examination. *Information Management & Computer Security*, *13*(4), 297–310. https://doi.org/10.1108/09685220510614425

Gupta, M., & Sharman, R. (Eds.). (2009). *Handbook of Research on Social and Organizational Liabilities in Information Security:* IGI Global. https://doi.org/10.4018/978-1-60566-132-2

Herriott, R. E., & Firestone, W. A. (1983). Multisite Qualitative Policy Research: Optimizing Description and Generalizability. *Educational Researcher*, *12*(2), 14–19. https://doi.org/10.3102/0013189X012002014

Hielscher, J., Menges, U., Parkin, S., Kluge, A., & Sasse, M. A. (2023). *"Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security*.

Hofstede Insights. (n.d.). Malaysia. *Hofstede Insights*. Retrieved 6 June 2022, from https://www.hofstede-insights.com/country/malaysia/

Hofstede Insights. (2022). Country Comparison. *Hofstede Insights*. https://www.hofstede-insights.com/country-comparison/

Horne, C. (2016). *Lack Of Cyber Security Knowledge Leads to Lazy Decisions from Executives*. The Conversation. http://theconversation.com/lack-of-cyber-security-knowledge-leads-to-lazy-decisions-from-executives-68065

Hsu, C. W. (2009). Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization. *European Journal of Information Systems*, *18*(2), 140–150. https://doi.org/10.1057/ejis.2009.7

Hu, Q., Hart, P., & Cooke, D. (2007a). The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004

Hu, Q., Hart, P., & Cooke, D. (2007b). The Role of External and Internal Influences on Information Systems Security: A Neo-Institutional Perspective. *The Journal of Strategic Information Systems*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004

Hwang, K., & Choi, M. (2017). Effects of Innovation-Supportive Culture and Organizational Citizenship Behavior On e-Government Information System Security Stemming From Mimetic Isomorphism. *Government Information Quarterly*, *34*(2), 183–198. https://doi.org/10.1016/j.giq.2017.02.001

IEEE Computer Society (Ed.). (1990). *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. Institute of Electrical and Electronics Engineers.

International Organization for Standardization. (n.d.-a). *ISO - ISO/IEC 27001—Information Security Management*. ISO. Retrieved 24 May 2022, from https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization. (n.d.-b). *ISO/IEC 27014:2020*. ISO. Retrieved 5 October 2022, from https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/40/74046.html

International Standard ISO/IEC 27000. (2018). *ISO/IEC 27000*.

IT Governance Institute. (2006). *Information Security Governance: Guidance For Boards of Directors and Executive Management*. IT Governance Institute. http://www.books24x7.com/marc.asp?bookid=30815

Jabatan Perdana Menteri, Malaysia. (2000). *Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan*. *3*. http://sgcert.org/policy-folder/AppendixA.pdf

Jarvenpaa, S. L., & Ives, B. (1991). Executive Involvement and Participation in the Management of Information Technology. *MIS Quarterly*, 205–227.

Jasperson, J. (Sean), Carte, T. A., Saunders, C. S., Butler, B. S., Croes, H. J. P., & Zheng, W. (2002). Review: Power and Information Technology Research: A Metatriangulation Review. *MIS Quarterly*, *26*(4), 397. https://doi.org/10.2307/4132315

Jeyaraj, A., & Zadeh, A. (2020). Institutional Isomorphism in Organizational Cybersecurity: A Text Analytics Approach. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 361–380. https://doi.org/10.1080/10919392.2020.1776033

Johnson, M. E., & Goetz, E. (2007). Embedding Information Security into the Organization. *IEEE Security & Privacy*, *5*(3), 16–24.

Johnston, A. C., & Hale, R. (2009). Improved Security Through Information Security Governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Kajava, J., & Anttila, J. (2006). *Senior Executives Commitment to Information Security—From Motivation to Responsibility*. 4.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Kaplan, B., & Maxwell, J. A. (2005). Qualitative Research Methods for Evaluating Computer Information Systems. In J. G. Anderson & C. E. Aydin (Eds.), *Evaluating the Organizational Impact of Healthcare Information Systems* (pp. 30–55). Springer-Verlag. https://doi.org/10.1007/0-387-30329-4_2

Karlsson, F., Astrom, J., & Karlsson, M. (2015). Information Security Culture—State-of-the-art Review between 2000 and 2013. *Information and Computer Security*, *23*(3), 246–285. https://doi.org/10.1108/ICS-05-2014-0033

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A Framework for Outsourcing IS/IT Security Services. *Information Management & Computer Security*, *14*(5), 403–416. https://doi.org/10.1108/09685220610707421

Kassarjian, H. H. (1977). Content Analysis in Consumer Research. *Journal of Consumer Research*, *4*(1), 8–18.

Katsikas, S. (2000). Health Care Management and Information Systems Security: Awareness, Training or Education? *International Journal of Medical Informatics*, *60*(2), 129–135. https://doi.org/10.1016/S1386-5056(00)00112-X

Kaur, K. (2016). Information Security Management of an Organization with a Focus on Human Perspective. *International Journal of Computer Techniques*, *3*(2). http://www.academia.edu/download/46356063/IJCT-V3I2P29.pdf

Kerlinger, F. N. (1973). The Nature of Research and Science. In *Foundations of Behavioral Research* (2nd ed., Vol. 1, pp. 1–19). Holt, Rinehart and Winston. http://journals.sagepub.com/doi/10.3102/0091732X001001005

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Khoo, B., Harris, P., & Hartman, S. (2010a). Information Security Governance of Enterprise Information Systems: An Approach to Legislative Compliant. *International Journal of Management and Information Systems*, *14*(3), 49–56.

Khoo, B., Harris, P., & Hartman, S. (2010b). Information Security Governance of Enterprise Information Systems: An Approach to Legislative Compliant. *International Journal of Management and Information Systems*, *14*(3), 49.

Kim, K., & Kim, J. (2015). A Role of Information Security Committee based on Competing Values Framework. *Proceedings of the 17th International Conference on Electronic Commerce 2015 - ICEC '15*, 1–4. https://doi.org/10.1145/2781562.2781600

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67. https://doi.org/10.2307/249410

Knapp, K. J. (2005). *A Model of Managerial Effectiveness In Information Security: From Grounded Theory to Empirical Test*. 222.

Knapp, K., Marshall, T., Rainer, R. K., & Morrow, D. (2006). The Top Information Security Issues Facing Organizations: What Can Government Do to Help? *Information Systems Security*, *15*(4), 51–58. https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95124.6

Kuhn, T. S. (1970). *The Structure of Scientific Revolutions* ([2d ed., enl). University of Chicago Press.

Landis, J. R., & Koch, G. G. (1977). The Measurement of Observer Agreement for Categorical Data. *Biometrics*, *33*(1), 159–174.

Lankton, N. (2016). *Board Involvement With IT Governance—Practically Speaking Blog*. http://www.isaca.org/Journal/Blog/Lists/Posts/Post.aspx?ID=314

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/j.bushor.2021.02.022

Leech, T. (2016). *Three Lines of Defense vs. Five Lines of Assurance*.

Lewin, K., Lippitt, R., & White, R. K. (1939). Patterns of Aggressive Behavior in Experimentally Created "Social Climates". *The Journal of Social Psychology*, *10*(2), 269–299. https://doi.org/10.1080/00224545.1939.9713366

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007a). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management.pdf. *MIS Quarterly*, *31*(1), 59–87.

Liang, Saraf, Hu, & Xue. (2007b). Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management. *MIS Quarterly*, *31*(1), 59. https://doi.org/10.2307/25148781

Lidster, W. W., & Rahman, S. S. M. (2018). Obstacles to Implementation of Information Security Governance. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE*

International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1826–1831. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00276

Linstone, H. A. (1989). Multiple Perspectives: Concept, Applications, and User Guidelines. *Systems Practice*, *2*(3), 307–331. https://doi.org/10.1007/BF01059977

MAMPU. (2022). MAMPU Department. *Laman Web Rasmi MAMPU*. https://www.mampu.gov.my/en/about-us/role-of-mampu-department/

MAMPU, MIMOS, CGSO, & CyberSecurity Malaysia. (2016). *Public Sector's Cyber Security Framework, Version 1.0*.

Merriam, S. B. (2009). *Qualitative Research: A Guide to Design and Implementation*. Jossey-Bass.

Merriam-Webster Dictionary. (n.d.). *Engagement Definition & Meaning—Merriam-Webster*. Retrieved 25 July 2022, from https://www.merriam-webster.com/dictionary/engagement

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology*, *83*(2), 340–363.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (Third edition). SAGE Publications, Inc.

Mishra, S. (2015). Organizational Objectives for Information Security Governance: A Value Focused Assessment. *Information and Computer Security*, *23*(2), 122–144. https://doi.org/10.1108/ICS-02-2014-0016

Mitroff, I. I., & Linstone, H. A. (1993). *The Unbounded Mind: Breaking The Chains of Traditional Business Thinking*. Oxford University Press.

Mokhtar Mohd Yusof, Ruzaina Wan Haniff, & Chua, C. O. (1998). *Implementing Information Systems Plan in Malaysian Government Organisation: A Multiple Perspective Framework*. 10.

Molok, N. N. A., Ahmad, A., & Chang, S. (2018). A Case Analysis of Securing Organisations Against Information Leakage Through Online Social Networking. *International Journal of Information Management*, *43*, 351–356. https://doi.org/10.1016/j.ijinfomgt.2018.08.013

Morse, J. M. (2000). Determining Sample Size. *Qualitative Health Research*, *10*(1), 3–5. https://doi.org/10.1177/104973200129118183

Moulton, R., & Coles, R. S. (2003). Applying Information Security Governance. *Computers & Security*, *22*(7), 580–584. https://doi.org/10.1016/S0167-4048(03)00705-3

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, *21*(2), 241–242.

MyGOV. (2022). *MyGOV - Keselamatan Siber Dan Tindak Balas Serta Pemulihan Bencana | Keselamatan Siber | Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)*. https://www.malaysia.gov.my/portal/content/30090?language=my

NACSA. (2022). *National Cyber Security Agency*. https://www.nacsa.gov.my

National Security Council. (2020). *Malaysia Cyber Security Strategy 2020-2024*. Prime Minister Department.

Nellis, R. (2003). *Creating an IT Security Awareness Program for Senior Management*. 18.

Nicho, M. (2018). A Process Model for Implementing Information Systems Security Governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ICS-07-2016-0061

Niekerk, J. F. V., & Von Solms, R. (2010). Information Security Culture: A Management Perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Official Portal of MSC Malaysia. (n.d.). Retrieved 14 June 2017, from http://www.mscmalaysia.my/what_is_msc_malaysia_status

Ogbanufe, O. (2021). Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. *Computers & Security*, *108*, 102340. https://doi.org/10.1016/j.cose.2021.102340

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1–28. https://doi.org/10.1287/isre.2.1.1

Othman Talib. (2018). *Analisis Data Kualitatif ATLAS.ti*.

Oxford Learner's Dictionary. (n.d.). *engagement noun—Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com*. Retrieved 25 July 2022, from https://www.oxfordlearnersdictionaries.com/definition/english/engagement?q=engagement

Patton, M. Q. (2002). Two Decades of Developments in Qualitative Inquiry: A Personal, Experiential Perspective. *Qualitative Social Work: Research and Practice*, *1*(3), 261–283. https://doi.org/10.1177/1473325002001003636

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37–49.

Pidd, M. (2003). *Tools For Thinking: Modelling in Management Science* (2nd ed). Wiley.

Posthumus, S., & Von Solms, R. (2004). A Framework for The Governance of Information Security. *Computers & Security*, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006

Ragu-Nathan, B. S., Apigian, C. H., Ragu-Nathan, T. S., & Tu, Q. (2004). A Path Analytic Study of The Effect of Top Management Support for Information Systems Performance. *Omega*, *32*(6), 459–471. https://doi.org/10.1016/j.omega.2004.03.001

Rahim, N. Z. Ab. (2009). *Multiple Perspectives of Open Source Software Appropriation in Malaysian Public Sector*. Universiti Teknologi Malaysia.

Rai, S., & Chukwuma, P. (2017). Information security function: Optimum reporting and organization structure. *EDPACS*, *56*(3), 19–24. https://doi.org/10.1080/07366981.2017.1355100

Razali, F. M., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/S2212-5671(15)01106-5

Rothrock, R. A., & Kaplan, J. (2018). *The Board's Role in Managing Cybersecurity Risks*.

Sa, M., & Saner, T. (2011). *Institutional Isomorphism Between the TRNC And Turkey For e-Government Strategy: What Encourages Spontaneous Isomorphism? 3*(1), 12.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information Security Conscious Care Behaviour Formation in Organizations. *Computers & Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Sajko, M., Hadjina, N., & Sedinic, I. (2011). *Information Security Governance and How to Accomplish It*. 6.

Santoro, M. D., & Chakrabarti, A. K. (2002). Firm Size and Technology Centrality In Industry–University Interactions. *Research Policy*, *31*(7), 1163–1180. https://doi.org/10.1016/S0048-7333(01)00190-1

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (Seventh Edition). Pearson Education.

Schinagl, S., & Shahim, A. (2020). What Do We Know About Information Security Governance?: "From The Basement To The Boardroom": Towards Digital Security Governance. *Information & Computer Security*, *28*(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business—A Skill-Building Approach* (7th Edition). Wiley.

Silic, M., & Back, A. (2014). Information Security: Critical Review and Future Directions for Research. *Information Management & Computer Security*, *22*(3), 279–308. https://doi.org/10.1108/IMCS-05-2013-0041

Simon, H. A. (1976). *Administrative Behavior—A Study of Decision-Making Processes in Administrative Organizations* (Fourth). The Free Press.

Singh, A. N., & Gupta, M. P. (2019). Information Security Management Practices: Case Studies from India. *Global Business Review*, *20*(1), 253–271. https://doi.org/10.1177/0972150917721836

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239. https://doi.org/10.1007/s40171-013-0047-4

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions. *ACM Sigmis Database*, *38*(1), 60–80.

SIRIM QAS International. (n.d.). ISO/IEC 27001 Information Security Management System (ISMS). *SIRIM QAS International Sdn. Bhd.* Retrieved 24 May 2022, from https://www.sirim-qas.com.my/our-services/management-system-certification-related-services/iso-iec-27001-information-security-management/

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems*, *51*, 100642. https://doi.org/10.1016/j.accinf.2023.100642

SME Corporation Malaysia. (2022). *SME Definitions*. http://www.smecorp.gov.my/index.php/en/policies/2020-02-11-08-01-24/sme-definition

Snape, D., & Spencer, L. (2003). The Foundations of Qualitative Research. In *Qualitative Research Practice: A Guide for Social Science Students and Researchers* (Vol. 41). SAGE Publications, Inc. http://choicereviews.org/review/10.5860/CHOICE.41-1319

Song, J. H. (1982). Diversification Strategies and the Experience of Top Executives of Large Firms. *Strategic Management Journal*, *3*(4), 377–380.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stake, R. E. (2006). *Multiple Case Study Analysis*. The Guilford Press.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Tejay, G. P. S., & Barton, K. A. (2013). *Information System Security Commitment: A Pilot Study of External Influences on Senior Management*. 3028–3037. https://doi.org/10.1109/HICSS.2013.273

Tobi, S. U. M. (2016). *Qualitative Research, Interview Analysis & NVIVO 11 Exploration*. ARAS Publisher.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Tony & Francis*, 1–30.

Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cybersecurity*, *2011*, 1–12. https://doi.org/10.5171/2011.726196

U.S. Small Business Administration. (n.d.). *Size standards*. Size Standards. Retrieved 30 May 2022, from https://www.sba.gov/federal-contracting/contracting-guide/size-standards#section-header-0

Veiga, A. da, Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining Organisational Information Security Culture—Perspectives from Academia and Industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Vidgen, R. (1996). *A Multiple Perspective Approach to Information System Quality*. University of Salford, UK.

Von Solms, B. (2001). Corporate Governance and Information Security. *Computers & Security*, *20*(3), 215–218. https://doi.org/10.1016/S0167-4048(01)00305-4

Von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

Von Solms, R., & Niekerk, J. van. (2013). From Information Security to Cyber Security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Von Solms, S. B. (2010). The 5 Waves of Information Security–From Kristian Beckman to the Present. *IFIP International Information Security Conference*, 1–8. http://link.springer.com/chapter/10.1007/978-3-642-15257-3_1

Von Solms, S. H. (Basie), & Von Solms, R. (2009). *Information Security Governance*. Springer US. http://link.springer.com/10.1007/978-0-387-79984-1

Walsham, G. (1995). The Emergence of Interpretivism in IS Research. *INFORMS, Vol. 6*(No. 4), 376–394.

Wang, H., Xu, H., Lu, B., & Shen, Z. (2009). Research on Security Architecture for Defending Insider Threat. *2009 Fifth International Conference on Information Assurance and Security*, 30–33. https://doi.org/10.1109/IAS.2009.53

Warkentin, M., & Johnston, A. C. (2008). IT Governance & Organizational Design for Security Management. In *Information Security—Policy, Processes, and Practices* (pp. 46–68). M. E. Sharpe, Inc.

Whitman, M., & Mattord, H. J. (2012a). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*, *11*(1), 97–111.

Whitman, M., & Mattord, H. J. (2012b). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*, *11*(1). http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15351777&AN=85627224&h=Xrrnr%2BcYUwfj9zldJ9IJ7SrqVjgj%2F4Tb%2BWKgGG1ngsYn5RsuWU6QWbHfgtPHQbl87p5DJtZj7E6tJa03hSs3Hg%3D%3D&crl=c

Williams, P. (2001a). Information Security Governance. *IT Governance Institute*, *6*(3), 60–70.

Williams, P. (2001b). Information Security Governance. *Information Security Technical Report*, *6*(3), 60–70.

Willis, J. (1995). A Recursive, Reflective Instructional Design Model Based on Constructivist-Interpretivist Theory. *Educational Technology Publications, Inc.*, *35*(6), 5–23.

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (Sixth Edition). SAGE Publications, Inc.

Young, R., & Jordan, E. (2008). Top Management Support: Mantra Or Necessity? *International Journal of Project Management*, *26*(7), 713–725. https://doi.org/10.1016/j.ijproman.2008.06.001

Yusuf, Y., Gunasekaran, A., & Abthorpe, M. S. (2004). Enterprise Information Systems Project Implementation. *International Journal of Production Economics*, *87*(3), 251–266. https://doi.org/10.1016/j.ijpe.2003.10.004

Zucker, K. J. (2002). From the Editor's Desk: Receiving the Torch in the Era of Sexology's Renaissance. *Archives of Sexual Behavior*, 6.

APPENDIX A

CASE STUDY PROTOCOL

Research project title:
Top Management Engagement in Information Security: Multiple-case Studies of Malaysian Public Sector

Researcher:
1. Rufizah Abdul Munir (Principle Investigator)
2. Asst. Prof. Dr. Shuhaili Talib (Supervisor)
3. Asst. Prof. Dr. Nurul Nuha Abdul Molok (Supervisor)

Part	Structure of case study protocol	Activities	Notes
I	Introduction to case study 1. Case study design 2. Case study question & propositions 3. Case study protocol establishment	The case study questions are formulated based on the following issue and problems: 1. *[Issue]* Information security practices are challenging to implement and appreciate throughout the organisation. 2. *[Problem]* The implementation of information security is often delegated to technical people from IT unit 3. *[Problem]* The involvement and participation shown by top management in driving information security initiatives are relatively low. 4. *[Problem]* Information security initiatives are handled as a one-time project instead of a continuous process and improvement.	
II	Data collection procedures 1. Identification & case study selection 2. Data collection plan	Selection of case study (multiple case studies): 1. Several cases have been identified 2. Number of targeted participants: up to 24 to 28 (approximately 7 participants for each case) 3. Potential participants for each case: a. 2 top management (CIO and ICTSO), 4 employees who involved in information security; or	

Part	Structure of case study protocol	Activities	Notes
		b. 2 top management (CIO and ICTSO), 2 employees, 2 internal ISMS auditor Data collection plan: 1. Request confirmation letter from DDPGR office. 2. Prepare and revise interview questions. 3. Concurrently, do initial contact with the organisation (to identify CIO, ICTSO and employees who involved in information security) 4. Draft and submit (by e-mail) official letter, project description and consent form to potential cases (target: 4 cases but there is a plan to contact other government agencies if targeted cases give negative feedback) 5. Conduct mock interviews with eight (8) participants and refine interview questions based on feedback 6. Follow-up e-mails and get approval. 7. Arrange the field visit and interview. Tentatively on January 2018 until February 2018. 8. Data collection 1 – interview, document review, observation 9. Data collection 2 – follow ups Instrument 1. Interviewer (key instrument) 2. Case study protocol 3. Interview questions template 4. Participants/Contact Summary form 5. Document Review Summary form 6. Observation Summary form 7. Voice recorder	
III	Case study questions	Organized based on research questions (RQ)/objectives (RO) and theme: 1. 3 RQ 2. 3 RO 3. Theme 1: General information (Demographic data) 4. Theme 2: Technical/External factor 5. Theme 3: Organisation/Societal factor 6. Theme 4: Personal/Individual factor	
IV	Outline for case study report	Verification of the propositions	
V	Case study analysis	1. Thematic analysis	

Part	Structure of case study protocol	Activities	Notes
		2. Within-case and cross-case analysis 3. Cognitive mapping 4. Document survey analysis	
VI	Recommendations	1. The findings 2. The result 3. The report/summary	

Adapted from Tobi (2016); Yin (2018)

APPENDIX B

CONFIRMATION LETTER FROM UNIVERSITY

الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

KULIYYAH OF INFORMATION AND COMMUNICATION TECHNOLOGY

Reference : IIUM/309/DDPG/C/01/2/G1616130 10th November 2017

TO WHOM IT MAY CONCERN

Dear Sir/Madam

LETTER OF CONFIRMATION

Name	:	**Rufizah binti Abdul Munir**
Matric No	:	**G1616130**
Nationality	:	**Malaysian**
Programme	:	**Doctor of Philosophy (Information Technology)**
Thesis Title	:	**"Top Management Involvement and Participation in Information Security: Multiple-case Studies of Malaysian Public Sector"**
Supervisor	:	**Asst. Prof. Dr. Shuhaili Talib**
Co-Supervisor	:	**Asst. Prof. Dr. Nurul Nuha Abdul Molok**
Chairman	:	**Assoc. Prof. Dr. Abdul Rahman Ahlan**

This is to confirm that Sr. Rufizah Binti Abdul Munir our student of Doctor of Philosophy (Information Technology) at Department of Information System, Kuliyyah (Faculty) of Information and Communication Technology, International Islamic University Malaysia, Malaysia.

This is also to confirm that Sr. Rufizah Abdul Munir is in the process of collecting her data for her thesis. She needs to collect data from your organization, therefore your co-operation will be highly appreciated.

Please do not hesitate to contact our office at +603-61965613/6404 (SR. NARIETA BUKHARI) or e-mail at narieta@iium.edu.my if you have any other enquiries on this matter.

Any assistance rendered to her is most appreciated. Thank you.

ASSOC. PROF. DR. ABD RAHMAN AHLAN
Deputy Dean (Postgraduate & Research)
Kulliyyah of Information and Communication Technology
International Islamic University Malaysia,

MS
CERTIFIED TO MS ISO 9001:2008
Registration No. AI 3074

Garden of Knowledge and Virtue

Office Address: Kuliyyah of Information and Communication Technology, International Islamic University Malaysia, Jalan Gombak, Selangor.
Mailing Address: Kulliyyah of Information and Communication Technology, P. O. Box 10, 50728 Kuala Lumpur, Malaysia.
Tel: +603 6196 5601 Fax: +603 61925179 Website: http://www.iium.edu.my/kict

APPENDIX C

CONSENT FORM

Consent form for the person participating in the following research project:

"Top Management Involvement and Participation in Information Security: Multiple-case Studies of Malaysian Public Sector"

Name of participant: _____

Name of investigator(s): Rufizah Abdul Munir

1. I consent to participate in this project and I have been provided with an invitation letter.
2. I understand that after I sign and return this consent form, it will be retained by the researcher.
3. I acknowledge that:
   (a) My participation in this research is voluntary. I may withdraw and discontinue participation at any time;
   (b) The project is for the purpose of research only;
   (c) I have been informed that the confidentiality of the information I provide will be safeguarded subject to any legal limitations;
   (d) I have been informed that, with my consent, the interview will be audio-recorded. I understand that all recordings will be stored at the International Islamic University Malaysia (IIUM) and will be destroyed after five (5) years following the last date of publication;
   (e) My name will be referred to by a pseudonym in any publications arising from the research;
   (f) I understand that any information I provide is confidential, and that, subject to the limitations of the law, no information that could lead to the identification of any individuals will be disclosed in any research reports or any publication to be written. However, due to small number of participants in this research project, there is a possibility that individuals, or agencies can be identified by contextual information; and
   (g) I have been informed that a copy of the research findings is available upon request from the researchers.

I consent to this interview being audio-recorded ☐ **Yes** ☐ **No** (Please tick)

I wish to receive a copy of the summary project report on research findings ☐ **Yes** ☐ **No** (Please tick)

Participant signature: _____ Date: _____

For further information, please contact:

Rufizah Abdul Munir
Principal Investigator
Department of Information Systems
Kulliyyah (Faculty) of Information & Communication Technology
E-mail: rufizah.munir@live.iium.edu.my

APPENDIX D

INTERVIEW CHECKLIST

Interview Checklist

Organization: _____
Date: _____

Before interview

☐ Opening – introduce myself, thank you for willing to participate
☐ Explain briefly about **research topic** – objectives: how info sec being practiced; how top mgmt. drive info sec; issues faced by top mgmt.
☐ Inform participant – interview will be conducted in **both** languages (Malay and English)
☐ Remind participant about **audio recorded**
☐ Remind participant about the **confidentiality** of the interview
☐ Inform participant – a copy of research findings is available upon request
☐ Participant sign the **consent form**
☐ Participant fill up the **short survey**

Pre-interview (while waiting for participant to fill up forms)

☐ **List of participants** – ask participant their category (to determine set of questions)
☐ Prepare **research questions, interviewee/contact summary form**
☐ Prepare **audio recorder**
☐ Ask participant if he/she has any questions before the interview starts

- **Interview starts** -

After interview

☐ Thank you and shall contact for further information (if any)
☐ Give **token of appreciation** to participant
☐ Ask participant to recommend staff/department for further investigation (document review)
☐ Do **document review**
  - ❍ Prepare **document review summary form**
  - ❍ Organization chart for ISG/information security platform, the members
  - ❍ Information security policy
  - ❍ Check minute meeting template if information security matters become fixed agenda
  - ❍ Others _____
    _____
    _____

☐ Fill up **observation summary form** (if any)
☐ Ask for a place to settle down

Reminder!

☐ Audio recorder has battery
☐ Give token of appreciation to contact person/gateway

Note(s)

_____
_____

APPENDIX E

DEMOGRAPHIC SURVEY FORM

DEPARTMENT OF INFORMATION SYSTEMS
KULLIYYAH (FACULTY) OF INFORMATION & COMMUNICATION TECHNOLOGY

"Top Management Engagement in Information Security: Multiple-case Studies of Malaysian Public Sector"

Mohon mengisi kajiselidik ini sebelum sesi temubual dijalankan.

Nama: .....

Jawatan: .....

Bahagian/Jabatan/Unit: .....

Agensi//Kementerian: .....

Tarikh temubual: .....

Untuk soalan-soalan di bawah, sila tandakan (✓) pada jawapan (satu atau lebih) yang bersesuaian dengan anda.

1. Lingkungan umur anda:
   - ❍ 20 – 30 tahun
   - ❍ 31 – 40 tahun
   - ❍ 41 – 50 tahun
   - ❍ 51 – 60 tahun
   - ❍ 61 dan ke atas

2. Berapa lamakah anda telah berkhidmat dalam sektor awam?
   - ❍ Kurang dari setahun
   - ❍ 1 – 3 tahun
   - ❍ 3 – 5 tahun
   - ❍ 5 – 10 tahun
   - ❍ Lebih 10 tahun

3. Berapa lamakah anda telah berkhidmat di agensi/jabatan/bahagian/kementerian ini?
   - ❍ Kurang dari setahun
   - ❍ 1 – 3 tahun
   - ❍ 3 – 5 tahun
   - ❍ 5 – 10 tahun
   - ❍ Lebih 10 tahun

1/3

4. Latarbelakang pendidikan anda *(tandakan semua yang berkenaan)*:
   - ☐ SPM
   - ☐ Diploma. Nyatakan bidang: ……
   - ☐ Ijazah. Nyatakan bidang: ……
   - ☐ Sarjana. Nyatakan bidang: ……
   - ☐ Doktor Falsafah. Nyatakan bidang: ……
   - ☐ Lain-lain. Sila nyatakan: ……

5. Anggaran jumlah kakitangan dalam organisasi: ……

6. Anggaran bilangan kakitangan yang terlibat/bertanggungjawab dalam tugasan berkaitan keselamatan maklumat: ……

7. Apakah peranan/jawatan anda berkaitan keselamatan maklumat di organisasi anda sekarang?
   - ☐ Tiada
   - ☐ Pengurusan atasan dalam tadbir urus keselamatan maklumat
   - ☐ CIO
   - ☐ ICTSO
   - ☐ Pengurus/Ketua di bahagian/jabatan/unit/kumpulan keselamatan maklumat
   - ☐ Pegawai/Kakitangan di bahagian/jabatan/unit/kumpulan keselamatan maklumat
   - ☐ Lain-lain. Sila nyatakan: ……

8. Di manakah anda mendapat pendedahan/pengetahuan berkenaan keselamatan maklumat? *(Tandakan semua yang berkenaan)*
   - ☐ Institusi pengajian (sekolah/kolej/universiti)
   - ☐ Pusat latihan (kerajaan/swasta)
   - ☐ Pejabat. Sila nyatakan: ……
   - ☐ Berkaitan dengan skop kerja sekarang
   - ☐ Pembacaan/Belajar sendiri
   - ☐ Tiada
   - ☐ Lain-lain. Sila nyatakan: ……

9. Adakah organisasi anda mendapat pensijilan keselamatan maklumat?
   - ❍ Tidak berminat mendapatkan pensijilan
   - ❍ Belum tetapi berminat mendapatkan pensijilan. Sila nyatakan nama pensijilan: ……
   - ❍ Sedang dalam proses pensijilan. Sila nyatakan nama pensijilan: ……
   - ❍ Telah mendapat pensijilan. Sila nyatakan nama pensijilan: ……
   - ❍ Telah mendapat pensijilan tetapi sudah luput. Sila nyatakan nama pensijilan: ……
   - ❍ Tidak pasti

10. Sila tandakan (✓) pada jawapan yang dirasakan paling sesuai dengan diri anda untuk perkara di bawah:

	Tiada	Asas *(Novice; Basic Knowledge)*	Pertengahan *(Intermediate; Developing)*	Banyak *(Proficient; Advanced)*	Pakar *(Expert)*
Pengetahuan tentang keselamatan maklumat					

11. Sila tandakan (✓) pada jawapan yang berkenaan untuk perkara di bawah:

	Tidak pasti	Tiada	Tiada tetapi sedang dalam proses pembangunan	Ada tetapi sedang dikemaskini	Ada dan sedang digunapakai
Organisasi anda mempunyai polisi/dasar keselamatan maklumat					

Jika ada, nyatakan nama polisi/dasar keselamatan maklumat: ……
……...

--- Kajiselidik tamat. Terima kasih atas kerjasama saudara/saudari meluangkan masa dalam mengisi kajiselidik ini ---

3/3

APPENDIX F

INTERVIEW QUESTIONS

TOP MANAGEMENT	INFORMATION SECURITY OFFICER	NON-SECURITY OFFICER
Part Two – Defining information security and the perception		
1) Can you describe the function of your department?	1) Can you describe the function of your department?	1) Can you describe the function of your department?
2) What do you understand about information security?	2) What do you understand about information security?	2) What do you understand about information security?
3) In your opinion, what is the importance of information security in organization?	3) In your opinion, what is the importance of information security in organization?	3) In your opinion, what is the importance of information security in organization?
Part Three – Information security role and governance		
4) What is the role of top management in ISG?	4) What is the role of top management including CIO in ISG?	4) What is the role of top management including CIO in ISG?
		5) Based on your observation, how does top management engage in information security here?
		6) What are the reasons for you to comply with the information security rules at work?
5) What about the role of CIO/ICTSO?		
6) Is there an appointment to top management / CIO / ICTSO in information security governance? Is there any briefing given?		
7) Who is responsible to develop info security policy?	5) Who is responsible to develop info security policy?	7) Do you know the existence of information security policy? If yes, how? If no, why?
8) In which stage of the policy development would the top management get involved in? Does the policy being reviewed before approval? How the revisions being made? Who is involved? What are the review criteria? How long does the review take?	6) Is the top management involved in designing an info sec policy as a guide to the policy contents? In which stage of the policy development would the top management get involved in? Does the policy being reviewed before approval? How the revisions being made? Who is involved? What are the review criteria? How long does the review take? If no review, why?	
9) How does the policy being communicated?	7) How does the policy being communicated?	
10) How top management take part in communicating the policy to the organization?	8) How top management take part in communicating the policy to the organization?	
	9) Normally, when there is an issue with information security, how is the solution and reporting method? (Discuss and finish at the subordinate level and informed up for approval, or take it	

TOP MANAGEMENT	INFORMATION SECURITY OFFICER	NON-SECURITY OFFICER
	straight up and wait for further instructions, or how?)	
	10) How top management segregate info sec responsibilities?	
	11) In your opinion, the direction of information security in the organization is determined by the top management or is given based on the segregation of those responsibilities and appointed for approval?	
	12) How top management monitor info sec efforts?	
11) Does the top management initiate info sec programs or suggested by respective department?	13) Does the top management initiate info sec programs or suggested by you and your team?	
12) How top management segregate info sec responsibilities?		
13) How top management monitor info sec efforts?		
14) How do you ensure info sec initiatives are aligned with organization's mission/vision/objectives?		
Part Four – Information security awareness, practices and initiatives		
15) What's your opinion regarding the level of info sec among the employees?		8) What's your opinion regarding the level of info sec among the employees? Part 3 Q8
16) Is there any resistance from the employees in incorporating info sec in their daily routine? Why and how do you cope with that?		
	14) In your opinion, the information security initiatives undertaken by you and your team are easy to implement and manageable throughout the organization? If yes, what are the reasons? Does top management involve in this? If not, why? Is it because lack of top management's support?	
17) How do you motivate the employees to comply with info sec policy?	15) How top management motivate you and the other employees to comply with info sec policy? Does it effective?	9) How top management motivate you and the other employees to comply with info sec policy? Does it effective? Part 3 Q6
		10) Have you ever attended a course, awareness program, briefing or training on information security? If yes, who is responsible to handle such program? Does the attendance is compulsory? What motivate you to attend such programs?

TOP MANAGEMENT	INFORMATION SECURITY OFFICER	NON-SECURITY OFFICER
		11) In addition to the information security awareness program that we discussed earlier, what other forms of information security is being made here? (email, memo, mail, etc)? Which unit in charge in disseminating such information? Does it help you to understand more about info sec? If no, do you there is lack of information being disseminated?
Part Five – Technical/External factor		
18) How do you see directives from the government/cabinet influence the involvement of top management in info sec governance?	16) How do you see directives from the government/cabinet influence the involvement of top management in info sec governance? How would they react? What they usually do?	12) How do you see directives from the government/cabinet influence the involvement of top management in info sec governance? How would they react? What they usually do?
19) How do you see achievements from peer ministries, particularly in info sec, influence the involvement of top management in info sec governance?	17) How do you see achievements from peer ministries, particularly in info sec, influence the involvement of top management in info sec governance? If yes, what would top management do? Do their involvement improved? If not, why do you think so?	13) How do you see achievements from peer ministries, particularly in info sec, influence the involvement of top management in info sec governance? If yes, what would top management do? Do their involvement improved? If not, why do you think so?
20) Security Audit – do you involved in the effort towards this audit? How and in which stage?	18) Security Audit – does top management involved in the effort towards this audit? How and in which stage? If not, why?	
21) Is there any other external factor that might influence you and top management to be involved in ISG?	19) Is there any other external factor that might influence top management to be involved in ISG?	14) Is there any other external factor that might influence top management to be involved in ISG?
Part Six – Organizational/Societal factor		
Does the board meeting have fixed agenda that discuss about info sec matters/issues? Which platform? Who are the members? Do you think top management are more involved in info sec when it is always being discussed?	20) Does the board meeting have fixed agenda that discuss about info sec matters/issues? Which platform? Who are the members? Does the outcome of the discussion always give impact towards the direction of info sec in your organization? If there is no fixed agenda, why do you think so?	15) Does the board meeting have fixed agenda that discuss about info sec matters/issues? Which platform? Who are the members? Does the outcome of the discussion always give impact towards the direction of info sec in your organization? If there is no fixed agenda, why do you think so?
	21) What do you think about the information security reporting (report) provided by you and your team? Usually, does the top management understand the reporting and issues raised by you and your team? If yes, how do you present the report? If not, why?	

TOP MANAGEMENT	INFORMATION SECURITY OFFICER	NON-SECURITY OFFICER
	22) In your opinion, does the top management concerned with the reporting presented by you and your team? Does it help top management in making an informed decision regarding information security?	
22) If you lead info sec initiative and succeed, have you ever been rewarded? What kind of reward? Do you feel more motivated to be involved in leading information security initiatives?	23) In your opinion, if there is an appreciation for the success of information security initiatives provided, do you see top management will be more eager to commit?	16) In your opinion, if there is an appreciation for the success of information security initiatives provided, do you see top management will be more eager to commit?
23) Do you have freedom of speech or freedom of doing things related to info sec governance? Does it influence your involvement in information security?	24) Based on your observation, top management have freedom of speech or freedom of doing things related to info sec governance? Does it influence their involvement in information security?	17) Based on your observation, top management have freedom of speech or freedom of doing things related to info sec governance? Does it influence their involvement in information security?
24) Is there any IT technology that help you in driving info sec? Do you think it helps you in ISG? Does it make you more involved in info sec?	25) Is there any IT technology that help top management in driving info sec? Do you think it helps them in governing info sec? Does it make top management more involved in info sec?	18) Is there any IT technology that help top management in driving info sec? Do you think it helps them in governing info sec? Does it make top management more involved in info sec?
25) Do you think organization size influence your involvement in driving info sec? Could you explain in the context of your organization?	26) Do you think organization size influence your top management involvement in driving info sec? Could you explain in the context of your organization?	19) Do you think organization size influence your top management involvement in driving info sec? Could you explain in the context of your organization?
26) Is there any other internal/organizational factor that might influence you and top management to be involved in ISG?	27) Is there any other internal/organizational factor that might influence top management to be involved in ISG?	20) Is there any other internal/organizational factor that might influence top management to be involved in ISG?
Part Seven – Personal/Individual factor		
27) Based on your experience, what do your views to work with older/younger colleagues? Does age factor influence one's involvement in ISG?	28) Based on your experience, what do your views to work with older/younger top management? Does age factor influence their involvement in ISG?	21) Based on your experience, what do your views to work with older/younger top management? Does age factor influence their involvement in ISG?
28) What about education background? Does your education background influence your involvement in ISG?	29) What about education background? Does top management education background influence their involvement in ISG? Could you see the differences?	22) What about education background? Does top management education background influence their involvement in ISG? Could you see the differences?
29) What about working in IT-related fields? Do you think IT environment influence your involvement in ISG?	30) What about the top management that used to be working in IT-related fields? Do you think IT environment influence their involvement in ISG?	23) What about the top management that used to be working in IT-related fields? Do you think IT environment influence their involvement in ISG?

TOP MANAGEMENT	INFORMATION SECURITY OFFICER	NON-SECURITY OFFICER
30) Do you think the length of your service in this organization influences your involvement in information security governance?	31) Do you think the length of top management service in this organization influences their involvement in information security governance?	24) Do you think the length of top management service in this organization influences their involvement in information security governance?
31) Is there any other personal factor that might influence you and top management to be involved in ISG?	32) Is there any other personal factor that might influence top management to be involved in ISG?	25) Is there any other personal factor that might influence top management to be involved in ISG?
Part Eight – Information security resources		
32) Does the top management provide financial allocation for information security?	33) Does the top management provide financial allocation for information security? If yes, does it being given priority? If no, why? What about resources other than financial?	
	34) Have you ever applied for financial security / information security related information rejected by top management? If yes, what were the reasons? If no, that means info sec has always been given priority by the top management?	
	35) Based on your experience, how top management addressing issues or cases of leakage of information or non-compliance with information security policies amongst employees?	26) Based on your experience, how top management addressing issues or cases of leakage of information or non-compliance with information security policies amongst employees? Part 9 Q26
	36) Based on observation, what is your view of CIO and top management in leading information security initiatives in your organization?	27) Based on observation, what is your view of CIO and top management in leading information security initiatives in your organization? Part 9 Q27
33) Other than financial allocation, what other allocations are provided by the top management in strengthening information security efforts in the organization?		
Part Nine - Issues and constraints		
34) In your opinion what are the issues, constraints or shortcomings faced by you and top management in driving information security here?	37) In your opinion what are the issues, constraints or shortcomings faced by top management in driving information security here?	28) In your opinion what are the issues, constraints or shortcomings faced by top management in driving information security here?
35) Based on your experience, have you and other top management segregate the responsibility of information security governance to other sections / IT unit and give them the freedom to determine the direction of info sec here?		

TOP MANAGEMENT	INFORMATION SECURITY OFFICER	NON-SECURITY OFFICER
36) MAMPU - How is the ministry / government agency's acceptance, especially the top management in any information security initiative brought by MAMPU?	38) MAMPU - How is the ministry / government agency's acceptance, especially the top management in any information security initiative brought by MAMPU?	
37) Can you share a little bit about the ongoing efforts of the organization in strengthening info sec?		
Closing		
38) Before we conclude this interview, based on your experience, is there any more factors that influence your involvement and participation in ISG, which has yet to be discussed?	39) Before we conclude this interview, based on your experience, is there any more factors that influence top management involvement and participation in ISG, which has yet to be discussed?	29) Before we conclude this interview, based on your experience, is there any more factors that influence top management involvement and participation in ISG, which has yet to be discussed?
39) After the discussion we have gone through, what is the main reason why you are motivated to be involved in driving information security?	40) After the discussion we have gone through, what is the main reason why top management are motivated to be involved in driving information security?	30) After the discussion we have gone through, what is the main reason why top management are motivated to be involved in driving information security?
40) What about the least dominant factor?	41) What about the least dominant factor?	31) What about the least dominant factor?

APPENDIX G

CONTACT SUMMARY FORM

Contact Summary Form

Organization: _____
Name: _____
Designation: _____

Contact Type:

- ☐ Site visit
- ☐ Telephone
- ☐ E-mail
- ☐ Text
- ☐ Other: _____

Contact Details (telephone/e-mail): _____
Date: _____

1. Important things or issues highlighted

2. Summary of information (received or failed to get)

3. New hunch/leads indicated by this contact

4. Further questions needed from this contact

5. Notes / Additional comments

APPENDIX H

OBSERVATION SUMMARY FORM

Observation Summary Form

Organization: _____

Venue: _____

Observation on:

- ☐ People: _____
- ☐ Environment: _____
- ☐ Other: _____

Date: _____

1. Difficulty/Issues in answering interview questions

2. Environment of the organization

3. Summary of the observation

4. Notes / Additional comments

APPENDIX I

DOCUMENT REVIEW SUMMARY FORM

Document Review Summary Form

Organization: _____

Accessed From:

- ☐ On site: _____
- ☐ Website: _____
- ☐ Other: _____

Contact Details (telephone/e-mail): _____

Date: _____

1. Name of the document

2. Importance of the document

3. Summary of the document

4. Notes/Additional comments

APPENDIX J

RESEARCH DESCRIPTION

الجامعة الإسلامية العالمية ماليزيا
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
يونيورسيتي إسلام انتارابغسا ملايسيا

RESEARCH PROJECT DESCRIPTION

Rufizah Abdul Munir (Principle Investigator)
Department of Information Systems
Kulliyyah (Faculty) of Information and Communication Technology (ICT)
Ph: +60 12 356 5956
Email: rufizah.munir@live.iium.edu.my

Asst. Prof. Dr. Shuhaili Talib (Supervisor)
Department of Information Systems
Kulliyyah (Faculty) of Information and Communication Technology (ICT)
Ph: +60 3 6196 5643
Email: shuhaili@iium.edu.my

Asst. Prof. Dr. Nurul Nuha Abdul Molok (Supervisor)
Department of Information Systems
Kulliyyah (Faculty) of Information and Communication Technology (ICT)
Ph: +60 3 6196 6430
Email: nurulnuha@iium.edu.my

Research Project Title: "Top Management Involvement and Participation in Information Security: Multiple-case Studies of Malaysian Public Sector"

Introduction

As someone who has vast experience in information security governance and management, we would like to invite you to participate in our study on the involvement and participation of strategic decision makers in Malaysian public sector. The aim of study is to gather expert feedback on how top management drive information security initiatives in organizations, what motivates their involvement and participation, and exploring issues faced by the top management, particularly related to information security governance. This project is funded by the Public Service Department of Malaysia, under the Federal Training Award (HLP).

What will I be asked to do?

Should you agree, we would ask you to participate in an interview of about 1 hour, to get your expert opinion on the governance of information security in Malaysian public sector organizations. In addition, we will ask broader questions around the involvement among top management in information security initiatives and the strategies in governing information security in government agencies. With your permission, the interview session would be audio-recorded so that we can ensure that we make an accurate record of what you say. Upon request, we can provide a copy of the recorded transcript to verify that the information is correct and/or request deletions. We estimate that the total time commitment required of you would not exceed 1.5 hours.

Department of Information Systems
Kulliyyah of ICT, International Islamic University Malaysia
T: +60 3 6196 5621 **F:** +60 3 6195 5179
W: http://www.iium.edu.my/kict

APPENDIX K

RESEARCH SUMMARY

RINGKASAN KAJIAN

Rufizah Abdul Munir (Principle Investigator)
Department of Information Systems
Kulliyyah (Faculty) of Information and Communication Technology (ICT)
Ph: +60 12 356 5956
Email: rufizah.munir@live.iium.edu.my

Asst. Prof. Dr. Shuhaili Talib (Supervisor)
Department of Information Systems
Kulliyyah (Faculty) of Information and Communication Technology (ICT)
Ph: +60 3 6196 5643
Email: shuhaili@iium.edu.my

Asst. Prof. Dr. Nurul Nuha Abdul Molok (Supervisor)
Department of Information Systems
Kulliyyah (Faculty) of Information and Communication Technology (ICT)
Ph: +60 3 6196 6430
Email: nurulnuha@iium.edu.my

Tajuk Kajian: "Top Management Engagement in Information Security: Multiple-case Studies of Malaysian Public Sector"

Topik dan ringkasan kajian

Secara umumnya, kajian ini menjurus kepada meneroka dan memahami peranan dan penglibatan pengurusan tertinggi dalam pentadbiran keselamatan maklumat *(information security governance)* melibatkan polisi, perancangan, pendekatan, peruntukan kewangan dan sumber, program/latihan, dan lain-lain. Dalam era digital dan kebergantungan bisnes kepada teknologi ICT terutamanya dalam sektor awam, maklumat terutamanya maklumat terperingkat merupakan aset yang sangat penting kepada sesebuah organisasi. Jika dulu, penyelesaian ke atas insiden keselamatan maklumat hanya tertumpu kepada aspek teknikal dan teknologi/ICT, namun kini penyelesaian insiden juga mengambil kira pendekatan secara holistik melibatkan manusia dari segi pentadbiran dan pengurusan keselamatan maklumat. Menyentuh soal pentadbiran, pengurusan tertinggi mempunyai peranan dan tanggungjawab yang sangat penting dalam dalam menentukan halatuju keselamatan maklumat dalam setiap organisasi. Justeru, kajian ini cuba mengenalpasti faktor-faktor yang mempengaruhi penglibatan pengurusan tertinggi dalam menerajui keselamatan maklumat di dalam [NAMA ORGANISASI], serta mengenalpasti isu-isu yang dihadapi oleh mereka.

Kajian ini akan cuba melihat pentadbiran keselamatan maklumat daripada sudut pengurusan tertinggi, pengalaman daripada kakitangan yang terlibat secara langsung dalam keselamatan maklumat, serta pandangan daripada warga [NAMA ORGANISASI] yang lain. Saya memberi jaminan bahawa topik temubual ini tiada melibatkan perkara-perkara yang terlalu teknikal.

Kaedah pengumpulan data (temubual, *document review* dan *observation*)

Temubual ini akan dijalankan secara individu (berasingan) yang melibatkan seramai lapan (8) orang peserta daripada [NAMA ORGANISASI]. Setiap temubual akan mengambil masa kira-kira satu (1) jam untuk setiap peserta bagi setiap sesi. Temubual ini bakal dijalankan secara *verbal* yang mana beberapa soalan akan dikemukakan oleh penyelidik kepada para peserta seperti peranan, pandangan dan pengalaman mereka berkaitan keselamatan maklumat yang diperoleh sepanjang mereka berkhidmat khususnya di [NAMA ORGANISASI] dan di sektor awam secara amnya. Saya mohon kebenaran untuk *audio-recorded* bagi tujuan *transcribing* dan analisa data. Sukacita dimaklumkan bahawa setiap maklumbalas yang diterima sepanjang temubual ini adalah sulit, dan identiti para peserta serta nama agensi dirahsiakan seperti yang diterangkan di dalam keterangan projek (rujuk lampiran *Research Project Description*). Hasil akhir kajian juga tidak sesekali mendedahkan identiti sebenar peserta serta agensi terlibat. Selain daripada temubual, saya juga memohon kebenaran pihak [NAMA ORGANISASI] untuk merujuk dokumen-dokumen seperti polisi keselamatan maklumat dan sebagainya bagi tujuan pemahaman dan mengukuhkan hasil kajian.

Cadangan peserta temubual

Bagi memudahkan pemilihan peserta di kalangan warga [NAMA ORGANISASI], izinkan saya memberi cadangan seperti berikut:

- (3 peserta) Pengurusan tertinggi yang terdiri daripada Setiausaha Bahagian/Pengarah dan ke atas:
  - CIO
  - Seorang pengurusan tertinggi
  - Seorang ICTSO
- (3 peserta) Pegawai berkhidmat dalam bidang keselamatan maklumat yang terdiri daripada:
  - Ketua unit keselamatan maklumat
  - Dua (2) orang pegawai di unit keselamatan maklumat
- (2 peserta) Pegawai dan kakitangan warga [NAMA ORGANISASI]
  - Seorang pegawai/kakitangan di bahagian IT
  - Seorang pegawai/kakitangan di bahagian bukan IT

Saya berharap agar cadangan ini dapat membantu pihak [NAMA ORGANISASI] dalam menyenaraipendek peserta temubual kajian. Walau bagaimanapun, sebarang penambahbaikan atau pembetulan ke atas cadangan peserta ini amatlah dialu-alukan.

Cadangan tarikh, masa, lokasi

Berdasarkan perancangan semasa, bulan Januari 2018 telah diperuntukkan untuk sesi temubual ke atas empat (4) agensi awam terpilih yang mana [NAMA ORGANISASI] merupakan salah satu daripada agensi tersebut. Penetapan tarikh, masa dan lokasi temubual adalah bergantung kepada kesesuaian oleh pihak puan. Sekiranya tidak keberatan, mungkin pihak puan boleh memberi cadangan dan perbincangan akan dilakukan dari semasa ke semasa berdasarkan kesesuaian

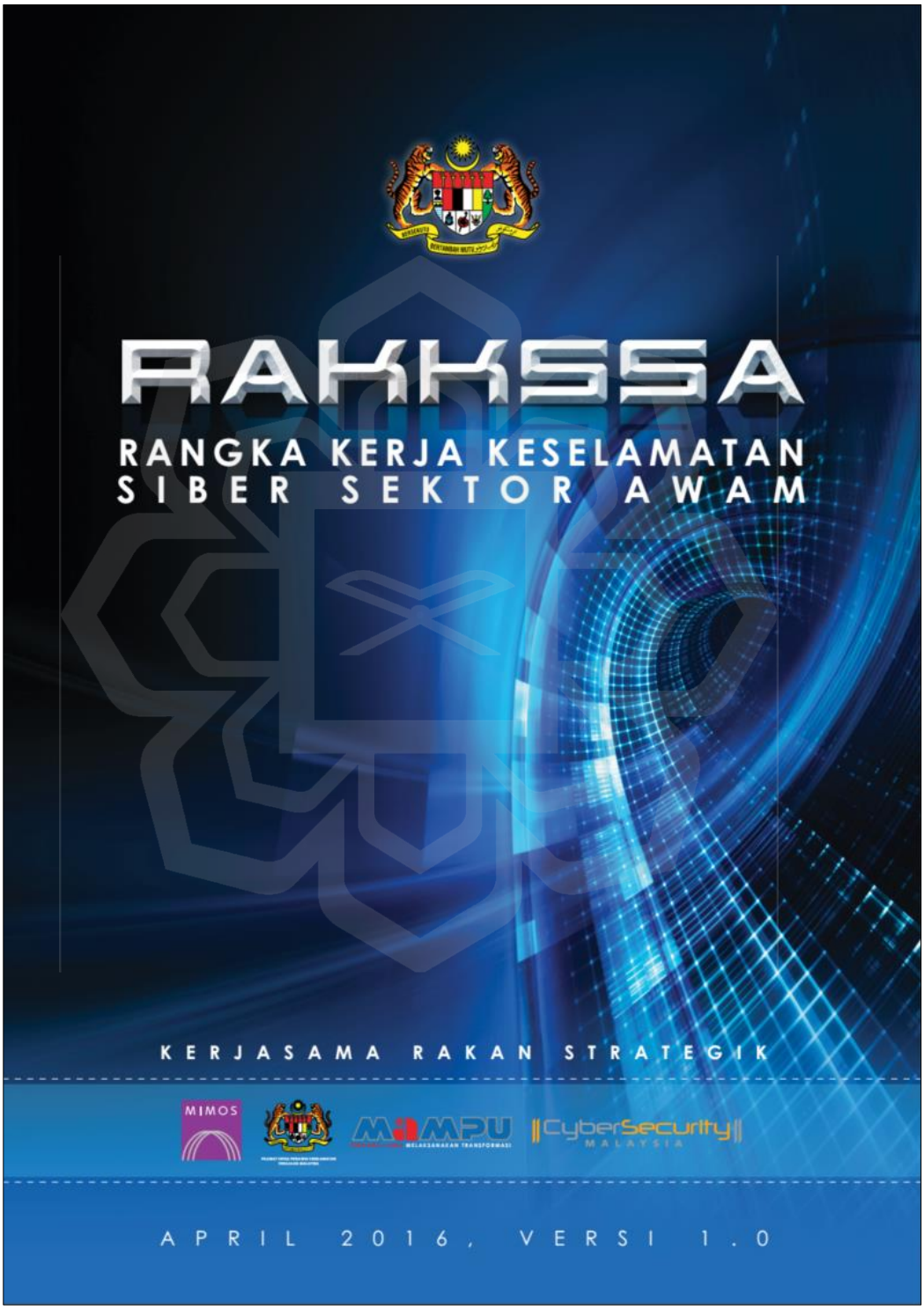
bersama. Walau bagaimanapun saya tiada halangan sekiranya cadangan tersebut perlu diberikan oleh pihak saya.

Pengedaran *consent form* dan *short survey form*

Consent form akan diedarkan kepada peserta-peserta yang terlibat. *Short survey form* berkenaan butiran diri peserta (nama, lingkungan umur, perjawatan, tempoh perkhidmatan, latarbelakang pendidikan, dll) juga akan disertakan. Bagi memudahkan semua pihak, saya bercadang untuk mengedarkan *consent form* dan *short survey form* tersebut ketika sesi temubual nanti (peserta akan mengisi kedua-dua borang sebelum sesi temubual bermula (anggaran masa adalah di antara 5 hingga 10 minit).

APPENDIX L

INFORMATION SECURITY FRAMEWORK



Kandungan

Akta Arkib Negara memberi mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

Bagi pelupusan data, sila rujuk seksyen 2.3.4.2.

2.4 Manusia

Kakitangan Jabatan, pembekal, pakar runding dan pihak-pihak yang berkepentingan, hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan.

Asas kecekapan pengguna hendaklah dibangunkan bagi semua pekerja dalam Jabatan.

2.4.1 Kompetensi Pengguna

Kompetensi pengguna termasuk:

- Kesedaran amalan terbaik keselamatan maklumat.

  Jabatan hendaklah memupuk amalan baik Keselamatan ICT dengan mewujudkan komunikasi ICT dan program kesedaran untuk memaklumkan kepentingan keselamatan ICT.

- Kemahiran menggunakan alat keselamatan

  Jabatan hendaklah menyediakan latihan yang mencukupi kepada kakitangan berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

2.4.2 Kompetensi Pelaksana

Kakitangan yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

Pegawai keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

- Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber
- Memenuhi keperluan pembelajaran berterusan
- Menimba pengalaman yang mencukupi dalam bidang keselamatan siber
- Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa

Pegawai Keselamatan ICT yang dilantik oleh Jabatan hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di Jabatan.

2.4.3 Peranan

Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

Kakitangan yang berperanan menguruskan aset hendaklah memastikan semua aset Jabatan dikembalikan sekiranya berlaku perubahan peranan.

Kakitangan yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti yang tersenarai dalam senarai aset dalam Nota Serah Tugas.

Kakitangan lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

APPENDIX M

GUIDELINES FOR THE EXTENSION OF RAKKSSA'S

COMPETENCY FOR TOP MANAGEMENT

Factor	Sub-factor	Competency Guidelines for Top Management
External	Regulatory forces	• Be updated and aware of information security statutes, regulations, and guidelines from the Cabinet, Chief Security Office (CGSO), MAMPU, NACSA or other higher authoritative bodies. • Be aware of and practice the roles and responsibilities of adhering to information security regulations, directives, *et cetera*. • Communicate and share information related to information security
	Audit compliance	• Be updated and aware of an information security audit in organisations • Take part in the audit process by providing input and responding to auditors' queries to fulfil the management commitment requirement clause • Expand existing audit scope to other departments other than IT Division • Be actively involved with the security activities by the information security team • Provide adequate resources, i.e. financial, and human resources for audit programs • Communicate and share information related to information security audits with the whole organisation
	Changes in security risk exposure	• Be updated and aware of information security risk exposure • Communicate with the information security team to tighten security measures • Provide a proactive approach by providing additional support and resources to the information security team, and monitor the implementation • Communicate and share information related to a security risk to the whole organisation
	Imitating good practice	• Be updated and aware of the development of information security initiatives in other ministries, agencies, and private sectors

Factor	Sub-factor	Competency Guidelines for Top Management
		• Communicate with the information security team to enhance security measures
Organisational	Information security risk awareness	• Practice a proactive approach to curb information security leakage by communicating with the information security team on the solutions • Constantly remind employees about the awareness of protecting information, especially when dealing with social media
	Reputation	• Set targets and direction to improve the reputation of the organisation by encouraging employees to take part in information security activities outside the organisation • Provide adequate resources and support to achieve the targeted plan
	Information security committee structure	• Be actively involved in formulating information security policies and directions and make known to the whole organisation • Ensure alignment between business objectives with risk and security management • Provide adequate security investments and resources for security programs • Define and assign responsibilities to non-information security stakeholders for collective participation in information security • Treat information security issues as significant as other business matters • Monitor and conduct timely assessments on information security programs and their implementation
	Culture	• Inculcate security culture by leading through example • Enforcement of the initiated information security rules and regulations
Personal	Informal education	• Have sound knowledge by doing self-exploration and reading about information security and its latest updates • Be actively involved in information security events outside organisations • Give proper briefing and training to any new CIO or security managers about their roles and responsibilities and appoint with the official appointment

Factor	Sub-factor	Competency Guidelines for Top Management
	On-the-job exposure	• Be actively involved in the current information security implementation by the information security unit • Establish a social network with the information security community
	Formal education	• Enrol in professional training and seminar on information security • Provide budget for information personalized security training and programs for all levels of employees to ensure the training programs fit their tasks

APPENDIX N

LIST OF PARTICIPANT DETAILS

No	Case	Pseudocode	Designation	Gender	Age	Length of Interview Session (hh:mm:ss)	Total Number of Interview Transcripts (page)
1	A1	A1TM1	CIO/Top Management	Female	51 – 60	01:08:51	22
2		A1IS1	Information Security Personnel	Male	51 – 60	01:23:16	29
3		A1NIS1	Non-Information Security Personnel	Male	41 – 50	00:32:58	10
4		A1NIS2	Non-Information Security Personnel	Male	41 – 50	00:58:55	18
5		A1NIS3	Non-Information Security Personnel	Male	41 – 50	00:45:23	13
6		A1NIS4	Non-Information Security Personnel	Male	41 – 50	00:39:00	14
7		A1NIS5	Non-Information Security Personnel	Male	41 – 50	00:21:41	8
8		A1NIS6	Non-Information Security Personnel	Male	51 – 60	00:49:08	16
9	A2	A2TM1	CIO/Top Management	Male	51 – 60	01:08:51	21
10		A2IS1	Information Security Personnel	Male	31 – 40	00:55:54	18
11		A2IS2	Information Security Personnel	Male	51 – 60	00:57:08	17
12		A2IS3	Information Security Personnel	Male	31 – 40	00:46:09	18
13		A2IS4	Information Security Personnel	Female	31 – 40	00:44:08	15
14		A2NIS1	Non-Information Security Personnel	Female	31 – 40	00:53:26	19
15		A2NIS2	Non-Information Security Personnel	Male	31 – 40	01:32:51	26
16		A2NIS3	Non-Information Security Personnel	Female	31 – 40	00:35:33	14
17	A3	A3TM1	Top Management	Female	51 – 60	01:28:41	25
18		A3IS1	Information Security Personnel	Female	51 – 60	00:43:53	13
19		A3IS2	Information Security Personnel	Female	31 – 40	01:06:27	24
20		A3NIS1	Non-Information Security Personnel	Male	31 – 40	00:50:21	14
21	A4	A4TM1	CIO/Top Management	Female	41 – 50	00:53:29	17

No	Case	Pseudocode	Designation	Gender	Age	Length of Interview Session (hh:mm:ss)	Total Number of Interview Transcripts (page)
22		A4IS1	Information Security Personnel	Female	41 – 50	00:54:14	19
23		A4IS2	Information Security Personnel	Female	31 – 40	01:02:12	20
24		A4IS3	Information Security Personnel	Male	41 – 50	01:17:43	26
25		A4IS4	Information Security Personnel	Male	20 – 30	00:41:20	17
26		A4NIS1	Non-Information Security Personnel	Male	51 – 60	01:29:11	12
27		A4NIS2	Non-Information Security Personnel	Male	41 – 50	00:54:04	21
						Grand Total:	**486**

APPENDIX O

RESEARCH PUBLICATIONS

Conference Proceeding:

1. Munir, R. A., Molok, N. N. A., & Talib, S. (2017). Exploring the Factors influencing Top Management Involvement and Participation in Information Security. *Pacific Asia Conference on Information Systems (PACIS)*, 65, 9. http://aisel.aisnet.org/pacis2017/65

2. Munir, R. A., Talib, S., Molok, N. N. A., & Ahmad, M. R. (2018). Responsibility-Value Alignment in Information Security Governance. *2018 International Conference on Information and Communication Technology for the Muslim World (ICT4M)*, 150–155. https://doi.org/10.1109/ICT4M.2018.00036

Journal Publication:

1. Munir, R. A., Talib, S., Molok, N. N. A., & Ahmad, M. R. (2023). Information Security Governance Issues in Malaysian Government Sector. *Journal of Information Systems and Digital Technologies (JISDT), 5(2), 1–18.*

2. Submitted to Journal: Computers & Security (2023)
   Title: Factors Influencing Top Management Engagement in Information Security
   Authors: Rufizah Abdul Munir, Shuhaili Talib, Nurul Nuha Abdul Molok, Mohd Ridzuan Ahmad, Steven Marcus Furnell