PROACTIVE FRAMEWORK FOR CYBER RISK IDENTIFICATION (PROCRIF)

NORAHANA BINTI SALIMIN

UNIVERSITI KEBANGSAAN MALAYSIA

PROACTIVE FRAMEWORK FOR CYBER RISK IDENTIFICATION (PROCRIF)

NORAHANA BINTI SALIMIN

PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT
FOR THE DEGREE OF
MASTER OF CYBER SECURITY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2023

KERANGKA PROAKTIF UNTUK PENGENALPASTIAN RISIKO SIBER (PROCRIF)

NORAHANA BINTI SALIMIN

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
SYARAT MEMPEROLEH
IJAZAH SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI
2023

DECLARATION

I hereby declare that the work in this project is my own except for quotations and summaries which have been duly acknowledged.

28 November 2023

NORAHANA SALIMIN
P105886

ACKNOWLEDGEMENT

Firstly, I praise Allah the Almighty for Bestowing His Mercy and Blessings upon me and for awarding me resilience and healthiness during this research.

I am very blessed to have Dr. Umi Asma' Mokhtar as my research supervisor for her guidance and support and for providing necessary information regarding the research. Also, for the motivation and belief in me, even when I doubted myself, to complete the research project within the timeline allocated by the faculty.

Moreover, I would like to express gratitude to my previous and current organizations for supporting my postgraduate journey; my earlier boss Dr. Maslina Daud and my current boss, Ts. Dr. Ismamuradi Abdul Kadir, for their kind support and understanding in giving me the flexibility to complete the research project. Also, to my colleagues for their encouragement and stimulating discussions.

I want to express my appreciation to my friends, fellow postgraduate students and support staff of FTSM for their help, friendship and advice throughout my research project.

Last but not least, my most profound appreciation to my darling husband, Mohd Adli Azaddin Samat; my precious son Noah Ahmad Mohd Adli Azaddin; my beloved parents, Aishah Abdul Hamid and Salimin Saijan; my beloved parents-in-law Zaiton Sukimi and Samat Moain; my dear supportive sister Norhidayu Salimin, my in laws Abdul Fattah Abdul Hamid, Nadia Abd Rani, Mohammed Feizal Samat and my dearest best friend, Norul Aina Amirah Ab Rahman. I am blessed with their support, care and sleepless nights being with me and getting me through this challenging journey, also for the inspiration and trust in me even when I was in my worst state of mind.

May Allah S.W.T grant you all the highest Jannah and blessings in your life.

ABSTRAK

Terdapat kebimbangan tentang sejauh mana risiko siber dikenal pasti dan sama ada pengenalpastian risiko mencukupi untuk menjangka potensi risiko daripada menjadi kenyataan akibat serangan oleh penggodam yang semakin kreatif dan canggih, khususnya dalam institusi kewangan. Walaupun institusi kewangan adalah industri yang dikawal selia dengan baik oleh badan kawal selia, kes insiden siber masih berleluasa. Penyelidikan ini bertujuan untuk membangunkan kerangka proaktif untuk pengenalpastian risiko siber dan instrumennya yang boleh menangani cabaran keselamatan siber untuk digunakan oleh institusi kewangan di Malaysia. Penyelidikan ini menggunakan pendekatan kualitatif melalui kajian kes tunggal institusi kewangan. Data dikumpul daripada semakan dokumen dalaman dan temu bual dengan pakar mengenai ancaman siber, pengenalpastian dan kawalan risiko siber. Kerangka yang dibangunkan disahkan oleh pakar bagi memastikan ia memenuhi objektif penyelidikan. Penyelidikan ini menerangkan pengenalpastian risiko siber yang dilihat pada aset maklumat, sumber ICT dan aset teknologi yang meliputi web, aplikasi mudah alih dan teknologi awan. Selain itu, penyelidikan ini membangunkan mekanisme kawalan risiko siber dari perspektif proaktif untuk mengurangkan risiko siber yang telah dikenal pasti. Kerangka proaktif untuk pengenalpastian risiko siber dan instrumennya telah dibangunkan untuk menggambarkan hubungan antara komponen pengenalpastian risiko siber dan komponen kawalan risiko siber dalam mengurangkan ancaman siber. Kesimpulannya, penyelidikan ini mempertingkatkan daya tahan keselamatan siber institusi kewangan dalam menghadapi ancaman siber, meningkatkan keyakinan pelanggan, memberi perspektif yang tepat terhadap landskap risiko siber, dan mengurangkan kebimbangan keselamatan apabila menggunakan teknologi tipikal dan baharu dalam persekitaran IT.

ABSTRACT

There is concern of how well cyber risks are being identified and whether the identification is sufficient to anticipate a potential risk from being materialised due to attacks by perpetrators are getting more creative and sophisticated, specifically in financial institutions. Even though financial institutions are a well-regulated industry by regulatory body, cases of cyber mishaps are nevertheless prevalent. This research intended to develop a proactive framework for cyber risk identification and its instrument which can address the challenges of cyber security to be used by financial institutions in Malaysia. This research employs a qualitative approach via a one case study of a financial institution. Data is collected from internal reviewed documents and interviews with experts on cyber threat, cyber risk identification and control. The framework developed is validated by experts ensuring it meets the research objectives. This research describes the cyber risk identification perceived on information assets, ICT resources and technological assets covering web, mobile application, and cloud. Additionally, this research has constructed the cyber risk control mechanism from a proactive perspective to mitigate the risk identified. A proactive framework for cyber risk identification and its instrument have been developed to illustrate the relationship between cyber risk identification component and cyber risk control component in diminishing cyber threats. In conclusion, this research improves cyber security resilience of financial institutions in facing cyber threats, increase customer confidence, give bird's-eye perspective of cyber risk landscape, and reduce security concerns when using typical and emerging technologies in IT environment.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

ADC	Alternative delivery channels
AI	Artificial intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
BB	Bangladesh Bank
BDN	Bayesian decision network
BNM	Bank Negara Malaysia
BOD	Board of Directors
BU	Business User
CCM	Cloud Controls Matrix
CERT	Computer Emergency Response Team
CIS	Centre for Internet Security
CISC	Cyber and Infrastructure Security Centre
CISO	Chief Information Security Officer
CKC	Cyber Kill Chain
CMMI	Capability Maturity Model Integration
CMS	Card management system
CRC	Cyber Risk Control
CRF	Cyber Resilience Framework
CRI	Cyber Risk Identification
CRMF	Cloud Risk Management Framework
CSA	Cloud Security Alliance
CSF	Cybersecurity Framework
CSH	Cybersecurity Strategic Headquarters
CSP	Cybersecurity Strategic Plan
DC	Datacentre
DDoS	Distributed Denial of Service

DFI	Development Finance Institution
DFIA	Development Financial Institutions Act
DHA	Department of Home Affairs, Australia
DLM	Digital Lighting Management
DLP	Data loss prevention
DNS	Domain Name System
DRC	Disaster Recovery Centre
EBA	European Banking Authority
EDR	Endpoint Detection and Response
e-KYC	Electronic Know Your Customer
FAST	Fully Automated System for Issuing/Tendering
FFIEC	Federal Financial Institutions Examination Council
FinTIP	Financial Sector Cyber Threat Intelligence Platform
FSA	Financial Services Act
FTSM	Fakulti Teknologi dan Sains Maklumat
GABV	Global Alliance for Banking on Values
HTTP	Hypertext Transfer Protocol
IAD	Internal Audit Department
ID	Identity
IFSA	Islamic Financial Services Act
IMF	International Monetary Fund
ISACA	Information Systems Audit and Control Association
ISP	Information Security Policy
KVM	Keyboard, Video, and Mouse
MAS	Monetary Authority of Singapore
MCIPD	Management of Customer Information and Permitted Disclosures
MFB	Microfinance Bank
ML	Machine Learning

MSP	Managed Service Provider
MyCERT	Malaysia Computer Emergency Response Team
NDR	Network Detection and Response
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OSFI	Office of Superintendent of Financial Institutions, Canada
OTP	One Time Password
OWASP	Open Worldwide Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PROCRIF	Proactive Framework for Cyber Risk Identification
RBI	Reserve Bank of India
RENTAS	Real-time Electronic Transfer of Funds and Securities System
RMF	Risk Management Framework
RMiT	Risk Management in Technology
ROI	Return of Investment
SBP	State Bank of Pakistan
SC	Security Commission Malaysia
SD-WAN	Software-Defined Wide Area Network
SDLC	Software Development Life Cycle
SEI	Software Engineering Institute
SG	Strategic Goal
SIEM	Security Information and Event Management
SOC	Security Operation Centre
SSDLC	Secure Software Development Life Cycle
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TRM	Technology Risk Management
TRMF	Technology Risk Management Framework

TTP	Tactics, Techniques, and Procedures
UKM	Universiti Kebangsaan Malaysia
VAPT	Vulnerability Assessment and Penetration Testing
WAF	Web Application Firewall
WIFI	Wireless Fidelity

CHAPTER I

INTRODUCTION

1.1 OVERVIEW

The digitisation of financial services, also driven by the COVID-19 pandemic, has increased cyber security threats globally. Cyber security threats in financial institutions have evolved from online financial transactions beyond cyber fraud. Cyber security risk usually implies to the risk of monetary deficiency, disruption of service to customers or reputational damage to the organisation due to IT system failure. Examples of attacks or incidents are ransomware attacks and data theft. According to a Gartner report (Moore 2022), the cyber security trends in 2022 include digital service provider chain risks, integration of vendor functions in the system, identity system defence and a more holistic security awareness program involving behavioural change. Cyber incident statistics (MyCERT 2022) from CyberSecurity Malaysia from January to September 2022 show that among the highest cases is fraud, with 3992 cases, followed by intrusion, with 597 cases.

Bank Negara Malaysia (BNM), the regulatory body for the banking, financial services and insurance sectors in Malaysia, has introduced a policy on risk management for technology, Risk Management in Technology (RMiT) (BNM 2023). All financial institutions must follow this policy in Malaysia, which includes aspects of risk management to deal with cyber threats. Strategies can be implemented to help financial institutions prepare to improve cyber resilience and adapt quickly to keep up with the ever-changing cyber landscape.

Even though financial institution is a well-regulated industry by regulators with the enforcement of cyber security policy due to their criticality in protecting our

financial matters, cases of cyber incidents are still evident (Baquero et al. 2022). Technology-driven business model, which includes the bank's emergence of digital services, has changed how banks operate. Digital services rely heavily on technology, which has increased the information and cyber risk to the financial institution. Therefore, financial institutions have more to safeguard and manage regarding cybersecurity governance (Tse 2022). There is concern about how well cyber risks are being identified and whether the identification is sufficient to anticipate a potential risk from being materialised due to attacks by perpetrators, which are getting more creative and sophisticated (Baquero et al. 2022).

Therefore, this research is intended to develop a proactive framework for cyber risk identification in addressing the cyber security challenges to be used by financial institutions in Malaysia.

1.2 BACKGROUND

Based on the annual report on cyber threats and forecasts for 2022 (FS-ISAC 2022) specific to the banking sector, the three highest threats are zero-day exploits, third-party or service provider attacks and ransomware. There is also an increase in the social engineering trend and fraud through phishing events using email, smishing using text messages and vishing using a telephone. 24% of cases were reported to be caused by personnel misled by phishing events. It is also reported that there are threats on organisations by Advanced Persistent Threat (APT) actors Distributed Denial of Service (DDoS), threatening organisations to pay a ransom if they do not want to be attacked.

The sudden increase in cybercrime worldwide has caused financial sector regulatory bodies across nations to tighten the regulation. The US Securities and Exchange Commission, the European Central Bank and the Monetary Authority of Singapore (MAS) have motioned that they propose to surge cyber security compliance responsibilities such as mandating cyber risk and incident disclosure, decrease the reporting period for cyber incidents and holding organisations accountable for cyber security measures by providers services (FS-ISAC 2022). Bank Negara Malaysia (BNM) has introduced a policy regarding risk management for technology, Risk

Management in Technology (RMiT) (BNM 2023). This policy covers governance, technology risk management, operations management, cyber security management, technology audits, awareness, and internal training. Meanwhile, MAS has introduced the Technology Risk Management Guideline (MAS 2021), which integrates technology risk management and oversight, IT project management and security-by-design, technology risk management framework, software application development and management, access control, IT service management, cryptography, IT resilience, cyber security operations, data and infrastructure security, IT audit, online financial services and cyber security assessment. Moreover, other countries such as Japan, the US, Canada, India, and Bangladesh have also established guidelines for their financial institutions regarding cyber security risk management.

Other than regulators, industries through standards bodies or leading organisations have also developed cyber security international standards documents and frameworks to guide organisations in managing their cyber risk.

All these national or organisation-level initiatives demonstrate the cruciality of protecting assets from cyber-attacks. With the emerging threats through more sophisticated and advanced cyber-attacks, an organisation needs to identify the risk upfront to implement the proper protection mechanism. Thus, safeguarding is vital to increase cyber resiliency in avoiding or surviving an attack.

1.3 PROBLEM STATEMENT

Even though financial institutions are a well-regulated industry with regulators enforcing cyber security policies due to the importance of protecting financial issues, cyber mishaps are still prevalent. There is concern about how well cyber risks are being identified and whether the identification is sufficient to anticipate a potential risk from being materialised due to attacks by perpetrators, which are getting more creative and sophisticated (Baquero et al. 2022). About 90% of security leaders agree that their organisation must address cyber risk more. Cyber risk mitigation challenges are utilising time to comply with regulatory requirements and awareness and training for employees (Foundry 2022). A comprehensive cyber risk management framework should be implemented, which includes strong governance, regular risk assessment and

control testing, remediation monitoring and awareness. It is necessary to establish a risk and control instrument for cybersecurity with references to globally accepted standards and regulatory requirements (Tse 2022).

In addressing the problem highlighted, this research intends to develop a proactive framework for cyber risk identification which can address the challenges of cyber security to be used by financial institutions in Malaysia. A framework is able to assist organisations to effectively and ease the process development to identify and mitigate risk at a level that an organisation can accept (Cisternelli 2022). Framework provides a graphic depiction or a road map for a suggested structure to implement improvements (Work Group for Community Health and Development at the University of Kansas 2014). It also reflects the foundation for a strategic course of action (Merzel & D'Afflitti 2011) based on research and experience (Kirby 2002). A framework is also feasible because it is created with the available and necessary resources in mind (Kirby 2002).

NIST Cybersecurity Framework (CSF) is a best practises document and industry norms framework (Almuhammadi & Alsaleh 2017). It is also more thorough when compared to other frameworks, such as ISO/IEC 27001 (Almuhammadi & Alsaleh 2017). NIST RMF lack of adoption and implementation (Maclean 2017). ISO 31000 is developed for a more broader audience which offers principles and generic guidelines (ISO 31000 2018) and not specific to cyber risk. Cybermaturity Platform is more focused on evaluating cyber maturity level of an organization (Brett 2021) which is not part of the research scope. CKC, OCTAVE and CIS Controls are emphasizing on cyber risk controls. Therefore, NIST Cybersecurity Framework (CSF) is the most suitable baseline framework for cyber risk management.

1.4 RESEARCH OBJECTIVES

This research intent to develop a proactive framework for cyber risk identification management for financial institutions in Malaysia. This research is based on three (3) primary objectives as follows:

1. Identify cyber risk on informational and non-informational assets covering web, mobile application, and cloud.
2. Identify control mechanisms in cyber risk treatment from a proactive perspective.
3. Develop a proactive framework for cyber risk identification.

1.5 RESEARCH QUESTION

This research is based on the following questions:

1. What is the cyber risk identification perceived on information assets, ICT resources and technological assets covering web, mobile applications, and cloud?
2. What is the cyber risk control mechanism from a proactive perspective?
3. How is the proactive framework for cyber risk identification management being developed?

1.6 RESEARCH SCOPE

The research scope covers the development of a proactive framework for cyber risk identification management aimed at financial institutions in Malaysia. Case studies refer to cyber incident cases in a bank in Malaysia (hereinafter known as Bank Z). The target audience for this framework is the financial institutions in Malaysia to identify a comprehensive coverage of cyber risk related to this industry. The risk identification coverage is on information assets, ICT resources and technological assets covering web, mobile application, and cloud. The research does not cover risk identification for technology such as IoT, blockchain and machine learning/artificial intelligence (ML/AI).

1.7 SIGNIFICANT OF RESEARCH

The study's results will benefit the financial institution's target group in ensuring compliance with the policies issued by BNM. Financial institutions can improve cyber

security resilience in combatting the growing cyber threats. It is well known that the financial institution is a lucrative target if hackers manage to penetrate the security infrastructure and steal customer data from financial institutions. This study will help financial institutions from losses and damaged business reputations, thus improving business management efficiency and income.

With increasing cases of fraud through phishing and other fraudulent methods, bank customers are increasingly afraid to use bank services online. The results of this study will increase customer confidence in the bank in ensuring that there is no leakage of individual information and loss of saved money.

Using the proactive framework for cyber risk identification management will benefit the financial industry in Malaysia in protecting the financial organisation from cyber-attacks and increase its cyber resiliency towards current and emerging threats.

This study provides a cyber risk identification framework of advanced technologies such as cloud computing in the IT infrastructure of financial institutions. Concerns about cyber risks when using advanced technology can be reduced with proper security controls to overcome cyber threats.

1.8 ORGANISATION OF THE PROJECT

This project organisation is divided into five chapters. Chapter I highlights the overview and background of this research. Then, the problem statement and research gaps are identified. The research objectives and scope are defined to solve the problem statement. Lastly, the significance of the research is briefly explained.

Chapter II explains a detailed literature review, which consists of definitions and concepts used throughout this report, current standards and guidelines on cyber risk and previous research on cyber risk management.

Chapter III describes the methodology used to obtain and validate research data to achieve the research objective.

Chapter IV discussed the results obtained through interviews with subject matter experts, case studies through document content analysis and expert validation of the research findings.

Chapter V describes the proactive framework for cyber risk identification in terms of its purpose, components, and framework validation by experts.

The last chapter, chapter VI, summarises the research results and suggests upcoming works.

1.9 CONCLUSION

Research on proactive framework for cyber risk identification management aimed at financial institutions in Malaysia is crucial as a preventive measure to protect the organisation from cyber-attacks. However, some issues and gaps are required to be addressed by this research through developing the respective framework. A bank in Malaysia is selected for data collection and case study. The following chapter will discuss how this research is being conducted to achieve its objectives.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

This chapter presents the definition and concept used and overview of the related works on cyber risk management. Besides that, this chapter includes previous studies that other researchers have conducted. Moreover, this chapter discovers different issues and challenges in the current cyber risk management frameworks and guidelines. Finally, this chapter highlights the conclusion of this section.

2.2 DEFINITION AND CONCEPT

2.2.1 Cyberspace

Cyberspace is defined as the composite ecosystem that comes from the interaction of users, software, and services on the Internet through the use of networks and technology apparatuses that are connected to it (ISO/IEC 27032 2012). However, the available definitions lacks neglecting causal relationships, are not grounded in the concept of constructiveness, and rely on vocabulary that is not well defined or has a clear physical meaning. Thus, any attempt to establish research questions to be solved is effectively compromised (Starodubtsev et al. 2020). Fedorov et al. (2021) proposes a new definition of cyberspace as following and perceive it as real space like land, air, or sea:

> Cyberspace is an artificial heterogeneous technological space with many supervision and process control agents at different tiers, the process of creating and operating which is not predetermined by the requirements of one control system, but functions in the interests of many heterogeneous control systems, some of which can be antagonistic, whereby its properties depend both on those

> of the cyberspace elements and the scope and properties of the processes being run in the interests of internal and external consumers.
>
> Source: Fedorov et al. (2021)

2.2.2 Information security and Information and communication technology (ICT) security

The information security and cyber security are frequently used interchangeably in recent articles about cyber security. Information exist in a many forms such as written, printed, electronic and can be transferred through mail or electronics medium (ISO/IEC 27002 2022). Information security is identified as safeguard of an asset which is information from potential destruction caused by numerous threats and vulnerabilities (Von Solms & Van Niekerk 2013) in accordance to Whitman and Mattord's:

> The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.
>
> Source: Whitman & Mattord (2022)

It is based on the confidentiality, integrity and availability (CIA) concept developed from computer security business (Whitman & Mattord 2022).

The safeguard of the definite technology-based systems on which information is frequently kept and/or transported is the focus of information and communication technology (ICT) security (Von Solms & Van Niekerk 2013). ICT security traits have additional concepts from information security, including non-repudiation, accountability, authenticity and reliability (Dhillon 2007). Therefore, ICT security is considered a subset of information security components (Von Solms & Van Niekerk 2013).

2.2.3 Cyber security

The definitions for cyber security are different from each community (i.e industry definitions, government and country definitions, academic definitions) (Schatz et al.

2017). Cyber security concerns assets in cyberspace or that can be impacted by cyberspace, including both informational and non-informational assets. Humans who can be impaired and physical properties that can be harmed utilising cyberspace, such as via mobile devices, are two examples of non-informational assets (Von Solms & Van Niekerk 2013). The improved definition proposed by Schatz which covers crucial elements for respective community:

> The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users.
>
> Source: Schatz et al. (2017)

The terms cyber security is associated but not similar to information security (Von Solms & Van Niekerk 2013). The linkage between cyber security, information security and ICT security is showed in Figure 2.1. Based on this figure, cyber security covers the fortification of cyberspace, data in electronic form, ICTs that sustenance cyberspace, and users of cyberspace in their individual, group, and nationwide capacities, including any of their benefits, concrete or immaterial, that are defenceless to cyberspace-originating attacks. Therefore, Cyber security goes well beyond the information and/or ICT security (Von Solms & Van Niekerk 2013).

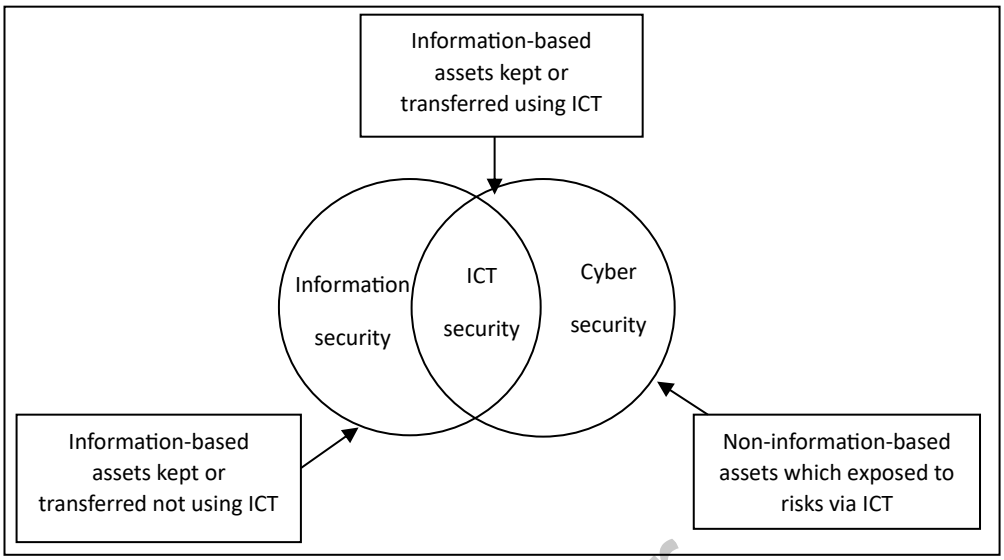

Figure 2.1 Linkage between cyber security, information security and ICT security
Source: Von Solms & Van Niekerk (2013)

2.2.4 Information security risk

According to NIST:

> Information security risk is the risk to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organisations, and the Nation due to the potential for unauthorised access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
>
> Source: NIST (2012)

It also defined as the potential effects on a company and its stakeholders because of risks and exposures related to the setup and usage of information systems and the surroundings in which those systems being setup (Gantz & Philpott 2013).

Risk associated with information security is quantified in terms of the chance of an incident and its effect (Katsikas 2013). The risk related to information security are comprised of threats, vulnerabilities, and impact. These three components are similar to event, probability and outcome (Talabis & Martin 2013). When thinking the probable outcomes of a security-related incident, information security risk coincides with

numerous more types of risk (Gantz & Philpott 2013). Therefore, the terms information risk can also overlap to cyber risk when we refer to the linkage of cyber security and information security (Von Solms & Van Niekerk 2013).

2.2.5 Cyber risk

Cyber security risk or cyber risk is described as any threat to the confidentiality, availability or integrity of information or facilities resulting from the use of information and communication technology (ICT) which have consequences of physical harm to people and property, economic or business interruption, and infrastructure failure. Natural catastrophes or human error can create cyber risk, resulting in cybercrime (such as blackmail and scam), cyberwar, or cyberterrorism (Eling et al. 2016). This definition of cyber risk is the most comprehensive term covering cyber risk sources, objects, and impact (Strupczewski 2021).

A more comprehensive cyber risk definition has been proposed by Strupczewski (2021) to streamline upcoming study in cybersecurity, which can also be adopted by cyber insurance market and policy maker for functional purposes. The proposed definitions are:

> Cyber risk is an operational risk associated with performance of activities in the cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term ’cyber risk’ also includes physical threats to the ICT resources within organisation.

Source: Strupczewski (2021)

The materialisation of the cyber risk as an event necessitating the need for response and recovery is known as cyber incident (NIST 2018a).

2.2.6 Cyber Risk Management

Cyber risk management is discovering, analysing, reviewing, and resolving organization's cyber security concerns (IT Governance UK 2023). Cyber risk management involved with risks triggered by cyber threats (Refsdal et al. 2015). In identifying cyber risk, the context establishment need to be established to understand where the attacks come from. It is called attack surface where attackers able to launch attack from numerous point to obtain access to the system and leak the confidential data or information out from the system (Refsdal et al. 2015). Assets that can be compromised by cyber-attack also falls under cyber risk management (McShane et al. 2021). Assets concern can be in the form of software, services and networks (Refsdal et al. 2015).

Due to cyber risk occurrences can have a significant, negative impact on businesses, organisations will need to set up a cyber risk approach, framework, group, or section (Gatzert & Schubert 2022). Long-term and short-term goals for cyber risk management can both be accomplished with proactive data collection and analysis of attackers (Marotta & McShane 2018).

2.2.7 Proactive and Reactive Cyber Security Techniques

Proactive cyber security technique is defined as IT resources such as firmware, software or hardware are designed with protections to prevent predicted attacks (Rowe & Gallaher 2006). It also defined as future attack plans are foreseen which influencing defence plans to integrate these insights (Colbaugh & Glass 2011). Several proactive technique that can be enforced are conducting cyber security awareness, periodically altering passwords and using intrusion detection system (Agamba & Keegnwe 2012; Miller 2016). Additionally, proactive technique is also about performing vulnerability scan to find vulnerabilities that can be eradicated by updating configuration of related IT or cyber elements (Y. Chen et al. 2018). Other cyber security deployment is also part of proactive technique such as firewalls, encryption, cryptography, biometrics, and digital certificates. With the emerging of technologies, more complex threats involving external and internal threats, instantaneous observation using sensors such as honeypot are being used to detect suspicious activities or attack (H. Saini 2016).

Reactive cyber security technique is responding to recognised materialised risks so that security vulnerabilities can be fixed quickly and successfully using generally accepted technology (Rowe & Gallaher 2006). Digital forensics is part of reactive technique where investigation of cyber incident is conducted by examining and analysing digital forensic evidence to find the attacker's attacks trail (Dimitriadis et al. 2020). Customary cyber threat intelligence (CTI) examines attack after they have occurred, producing reactive technique (Sagar Samtani, Ryan Chinn, Hsinchun Chen 2017). However, recent technology has expanded the function of CTI to become a proactive mechanism in detecting potential threats through gathering and scrutinising data from global covert hackers such as Dark Web (Basheer & Alkhatib 2021; Sagar Samtani, Ryan Chinn, Hsinchun Chen 2017).

Proactive measures and assessment of probable risks are necessary to encounter vulnerabilities in the cyber space (Perumal et al. 2018). Proactive cybersecurity technique will transform how we perceive threats (H. M. Chen et al. 2017).

This study uses proactive technique because proactive technique is more adequate to effectively address risk and that businesses should adopt a more proactive strategy for cybersecurity (EY 2014).

2.2.8 Financial Institutions

According to Bank Negara Malaysia (BNM), financial institution is referring to registered person/organisation that abide to Financial Services Act 2013 (FSA), Islamic Financial Services Act 2013 (IFSA) and Development Financial Institutions Act 2002 (DFIA), e-money issuer and operator of selected payment system which includes conventional banking, Islamic banking, insurance, takaful, development financial institutions, money service business and payment systems (BNM 2023). For Monetary Authority of Singapore (MAS), financial institutions covers banking, capital markets, insurance and payments segments (MAS 2023). While in Canada, financial institution includes banks, trust and loan businesses, insurance businesses, cooperative credit groups, familial welfare organisations and private retirement fund (OSFI 2022b). For Pakistan, financial institution refers to commercial banks, Islamic banks, Development Finance Institutions (DFIs) and Microfinance Banks (MFBs) (SBP 2017).

However, in Malaysia and Singapore, Financial and Technology innovation (FinTech) organisation that provides innovative solutions for financial services (Vučinić & Luburić 2022) is not governed by specific regulation under the respective regulatory bodies. The current regulation that applies to typical financial institutions like banks and insurance companies may apply to FinTech if the service provided by the FinTech falls under the regulation scope (Abdullah & Basirun 2022; Kin & Gaw 2022). Netherlands, even though is a country which strongly supported FinTech development, also has no special regulations for this type of establishment (Vervuurt & Ven 2022). Japan Regtech (Regulatory Technology) has not yet been established. However, its regulatory body would enhance it under assessment and strategic initiatives (Kawai et al. 2022).

For certain countries, FinTech is treated like other financial institutions and regulated under certain regulations. In the USA, FinTech is governed by federal, state regulation and regulatory bodies (Lorentz & Kost 2022). In Australia, FinTech rising financial services regulatory and legislative requirements are embedded into the current financial service structure (Reeves et al. 2022). Mexico has enacted the law to regulate FinTech, known as “Fintech Law” in 2018 (Lazcano et al. 2022).

Since this research uses case studies in Malaysia, definition of financial institutions by BNM will be used throughout this research.

2.3 CYBER RISK MANAGEMENT FRAMEWORKS

This section describes the existing cyber risk management frameworks from international standards organisation and well-known organisation. Analysis is then conducted on the existing cyber risk management frameworks to find gaps or issues arising.

2.3.1 Analysis on Existing Cyber Risk Management Frameworks

Information security standards are the basis of cyber risk management frameworks. It is suggested by (Biener et al. 2015; Eling & Schnell 2016) to utilise specifications such

as ISO/IEC 27001 and US NIST Framework. Other cyber risk frameworks by well-known organisations are also referred to as Table 2.1.

Table 2.1 Cyber Risk Management Frameworks

Framework	Highlighted areas	Reference	Framework Component/Element
Cybersecurity Framework	The National Institute of Standards and Technology (NIST) has produced a Cybersecurity Framework which is a method for overseeing cybersecurity risk. It consists of Framework Core, which explains common cybersecurity practises, objectives, and relevant references across critical infrastructure sectors. Framework Core consist of five functions: Identify, Protect, Detect, Respond and Recover.	(NIST 2018a)	Identify, Protect, Detect, Respond, Recover.
Risk management framework (RMF)	NIST has produced a risk management framework for information systems and organisation to provide any organisation a comprehensive, adaptable, repeatable, and measurable methods to manage information security and privacy risk for systems and organisations. The methods comprised of Prepare, Categorise, Select, Implement, Assess, Authorise and Monitor.	(NIST 2018b)	Prepare, Categorise, Select, Implement, Assess, Authorise, Monitor.
ISO 31000	The International Organization for Standardization (ISO) has produced a standards document for risk management principles, a framework, and a procedure that an organisation can use.	(ISO 31000 2018)	Leadership and communication, Integration, Design, Implementation, Evaluation, Improvement.
ISO/IEC 27001	The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) has produced an information security management system requirement which includes creating, putting into practise, sustaining, and enhancing an information security system for an organisation.	(ISO/IEC 27001 2022)	Organizational, People, Physical, Technological
ISO/IEC 27005	ISO/IEC has produced a guideline for implementing information security risks management actions such as risk assessment and remedy.	(ISO/IEC 27005 2022)	Context establishment, Risk assessment, Risk treatment, Risk acceptance,

to be continued …

… continuation

			Risk communication and consultation, Risk monitoring and review
Cyber Kill Chain (CKC)	Lockheed Martin has produced a risk management framework consisting of of seven stages/chains for detecting and preventing online intrusion. It imitates the attackers attacking steps to intrude an organisation.	(Martin 2009)	Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and control, Actions on objective, Monetization.
Cybermaturity Platform	CMMI Institute has produced a risk management method to develop enterprise cyber maturity by assessing, managing, and mitigating cybersecurity risk. The Cybermaturity Platform performs a security gap analysis to compare current maturity to goal maturity and prioritises security initiatives based on the organisation's cybersecurity risk outlines to construct roadmap based on risk.	(ISACA 2020)	Model, Adoption Guidance, Systems and Tools, Training and Certification, Appraisal Method
OCTAVE, OCTAVE Allegro	Computer Emergency Response Team (CERT) Division of Software Engineering Institute (SEI), Carnegie Mellon University has produced Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) strategic assessment grounded on risk. OCTAVE assists in the identification and rating of critical information technology assets, the assessment of threats to those assets, the evaluation of vulnerabilities and their impacts, and the formulation of security priorities to lessen the risk associated with those assets. OCTAVE Allegro is an improved version to ease the implementation of the framework in an organisation. OCTAVE Allegro offers a broad assessment of an organization's operational risk environment in a workshop-style collaborative setting without the necessity for an expertise of risk assessment.	(Richard A. Caralli, James F. Stevens, Lisa R. Young 2007; SEI 2005)	Establish Drivers, Profile Assets, Identify Threats, Identify and Mitigate
CIS Controls	Centre for Internet Security (CIS) has produced a set of endorsed cyber defence measures that offer precise, implementable solutions to thwart today's prevalent and hazardous threats.	(CIS 2019)	Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection,

to be continued …

… continuation

	The CIS uses Implementation Groups (IGs), which is like NIST Cybersecurity Framework execution stages. The IGs are envisioned to help organisations in categorising themselves per their rank of cybersecurity maturity, prioritising the deployment of controls, and creating a successful cybersecurity programme.	Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, Penetration Testing

2.3.2 Baseline Framework for Cyber Risk Management

NIST Cybersecurity Framework (CSF) is a best practises document and industry norms framework (Almuhammadi & Alsaleh 2017). It is also more thorough when compared to other frameworks, such as ISO/IEC 27001 (Almuhammadi & Alsaleh 2017). NIST RMF lack of adoption and implementation (Maclean 2017). ISO 31000 is developed for a more broader audience which offers principles and generic guidelines (ISO 31000 2018) and not specific to cyber risk. Cybermaturity Platform is more focused on evaluating cyber maturity level of an organization (Brett 2021) which is not part of the research scope. CKC, OCTAVE and CIS Controls are emphasizing on cyber risk controls. Therefore, NIST Cybersecurity Framework (CSF) is the most suitable baseline framework for cyber risk management.

CSF is a method for overseeing cyber security risk. It consists of Framework Core, which explains common cyber security practises, objectives, and relevant

references from a variety of essential infrastructure areas. Framework Core contains five components: Identify, Protect, Detect, Respond and Recover (NIST 2018a) as illustrated in Figure 2.2:

1. **Identify** - To govern cyber security risk to systems, assets, data, and resources, the organisation required to develop the needed knowledge on their current systems, assets, data, and resources.
2. **Protect -** Create and implement the appropriate safeguards to ensure the supply of critical infrastructure services.
3. **Detect -** Create and execute the necessary events to recognise the existence of a security incident.
4. **Respond -** When confronted with a detected security occurrence, develop, and put into practise the required actions.
5. **Recover -** Create and implement the necessary resilience-building measures and any necessary measures to reinstate any abilities or facilities that were impacted by a security event.

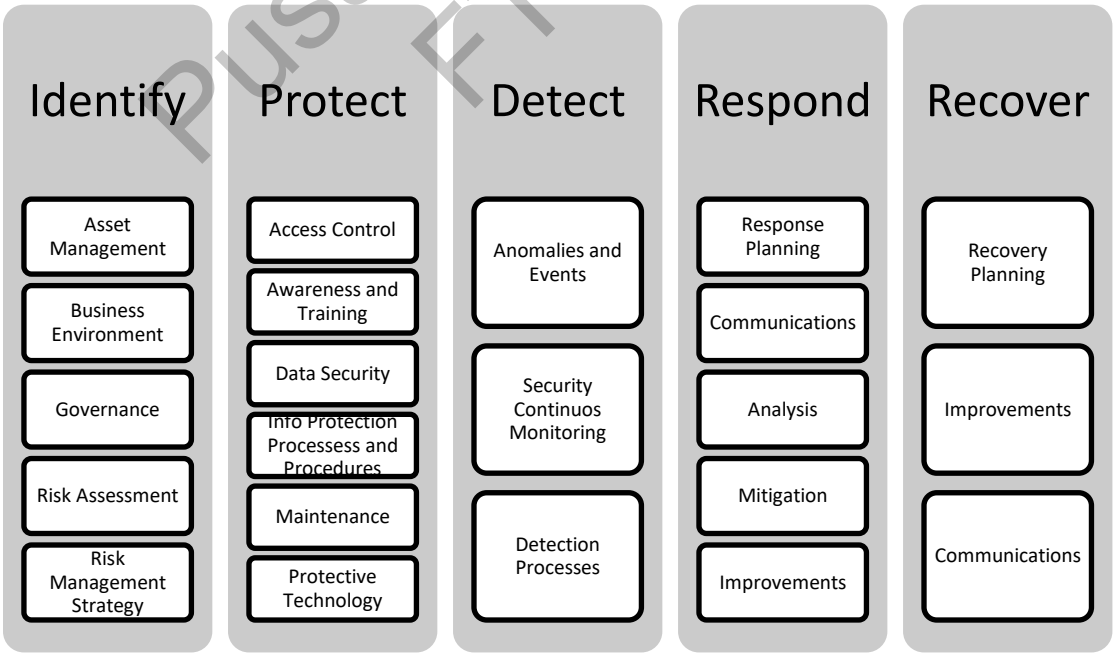

Figure 2.2 NIST Cybersecurity Framework

Source: NIST (2018a)

Based on CSF, Identify, Protect and Detect components will be adapted as baseline framework for proactive cyber risk identification. Identify component from CSF will be used as baseline framework for development of Cyber Risk Identification component in the proactive framework. Meanwhile, Protect and Detect components from CSF will be applied for development of cyber risk control component in the proactive framework.

However, CSF is not exhaustive to cover every information security-related process that some of those framework's cover. It is lacking the cyber security maturity level measurement (Almuhammadi & Alsaleh 2017). One of the maturity level measurement domains proposed by (Almuhammadi & Alsaleh 2017) is assessing security risk under risk management. Therefore, it is central to recognize security risk and measure it to uphold the required security posture for an organisation (Almuhammadi & Alsaleh 2017). However, maturity level measurement is not part of the research scope.

Additionally, most of the current cyber risk management standards are impromptu activities taken with no awareness of the risk driving factor. A better strategy to lessen the effects of technological and cyber risks is by considering non-technical factors like human behaviour as it typically plays a role in technological and cyber incidents (Uddin et al. 2020). This perspective is also supported by Kosub (2015), stating all stakeholders i.e. workers, suppliers, customers need to be aware of the cyber risks for effective cyber risk management.

Most current cyber risk management standards are also not specifically focusing on emerging technology risks such as cloud, the Internet of Things (IoT), blockchain, artificial intelligence (AI) (Basori & Ariffin 2022; Fischer 2017; Lee 2020).

The benefits of proactive framework are more adequate to address risk effectively (EY 2014), transform how we identify threats (H. M. Chen et al. 2017) and solve vulnerabilities in cyber space (Perumal et al. 2018).

2.4 CYBER RISK MANAGEMENT GUIDELINES

This section describes the existing cyber risk management guidelines from different countries from Asia Pacific, Europe, Australia, the US, and Canada. The analysis is then conducted on the existing cyber risk management guidelines to find gaps or issues.

2.4.1 Analysis of Cyber Risk Management Guidelines

Cyber risk management guidelines are different for each country. Table 2.2 specified guidelines on cyber risk related to the financial sector in distinct nations.

Table 2.2 Guidelines on cyber risk related to the financial sector in distinct nations.

Country	Highlighted areas	Outcome	Reference
Australia (C1)	The Department of Home Affairs, Australia (DHA) produced Australia's Cyber Security Strategy 2020. The strategies incorporate (a) Actions by businesses in terms of improving baseline security for critical infrastructure, providing secure products and services, growing a skilled workforce, block malicious activity and (b) Actions by the community in terms of accessing and applying guidance and information on cyber security, make wise purchasing choices, report cybercrime and accessing support when required. Meanwhile, the Cyber and Infrastructure Security Centre, Department of Home Affairs (CISC) produced a risk management program that covers risks on physical and natural, cyber and information security, personnel, and supply chain.	Cyber Security Strategy	(CISC 2022; DHA 2020)
Bangladesh (C2)	The Bangladesh Bank (BB) produced guidelines on ICT security for banks and non-bank financial institutions. The guidelines incorporate (a) ICT security management, (b) ICT risk management, (c) ICT service delivery management, (d) Infrastructure security management, (e) Access control of information systems, (f) Business continuity and disaster recovery management, (g) Acquisition and development of information systems, (h) Alternative delivery channels (ADC) security management, (i) Service provider management and (j) Customer education.	ICT Security Guidelines	(BB 2015)

to be continued …

… continuation

Canada (C3)	The Office of Superintendent of Financial Institutions Canada produced technology and cyber risk management guidelines. The guidelines incorporate (a) Governance and risk management, (b) Technology operations and resilience and (c) Cyber security.	Technology and cyber risk management guidelines	(OSFI 2022a)
Europe (C4)	The European Banking Authority (EBA) produced a final report on ICT and security risk management guidelines. The guidelines incorporate (a) Governance and strategy, (b) ICT and security risk management framework, (c) Information security, (d) ICT operations management, (e) ICT project and change management, (f) Business continuity management and (g) Payment service user relationship management.	ICT and security risk management guidelines	(EBA 2019)
Group of Seven (G7) (C5)	The Group of Seven (G7), which consists of leading industrial countries (Britain, Canada, France, Germany, Italy, Japan, and the United States), produced guidelines on cybersecurity for the financial sector. The guidelines incorporate (a) Cybersecurity Strategy and Framework., (b) Governance, (c) Risk and Control Assessment, (d) Monitoring, (e) Response, (f) Recovery, (g) Information Sharing and (h) Continuous Learning.	Cybersecurity Guidelines	(G7 2016)
India (C6)	The Reserve Bank of India (RBI) produced guidelines on information security, electronic banking, technology risk management and cyber frauds in 2011. The guidelines incorporate (a) IT governance, (b) Information security, (c) IT operations, (d) IT services outsourcing, (e) Information security audit, (f) Cyberfraud, (g) Business continuity planning, (h) Customer education and (i) Legal issues. In 2016, RBI published an extension of the guideline on cyber security framework to increase the banking system's resiliency in dealing with cyber risks. The guidelines incorporate (a) Cyber security policy, (b) Cyber security strategy, (c) Cyber Security Organization, (d) Cyber Risk / Gap Assessment, (e) Security testing, (f) Network and Database Security, (g) Physical & Environmental Security, (h) Third Party Risk Management, (i) Cyber Security Awareness, (j) Cyber Crisis Management Plan, (k) Cyber Security Operation Centre and (l) Incident Response & Management.	Guidelines on information security, electronic banking, technology risk management and cyber frauds	(RBI 2011, 2016)

to be continued …

… continuation

Japan (C7)	The Cybersecurity Strategic Headquarters (CSH) produced guidelines for establishing safety principles for ensuring the information security of the critical infrastructure. The guidelines incorporated (a) Plan: Organisation's situation in the external and internal environment and stakeholder's requirement, leadership, risk management, human resources development, awareness, and communication, (b) Do: Adoption and operation of information security measures, response and implementation of exercises and training, (c) Check: Monitoring, audits and review by management, and (d) Act: Corrective measures and continuous improvement.	Information Security Guidelines	(CSH 2019)
Malaysia (C8)	The Central Bank of Malaysia or Bank Negara Malaysia (BNM) produced technology risk management guidelines (RMiT). The guidelines incorporate (a) Governance, (b) Technology risk management, (c) Technology operations management, (d) Cybersecurity management, (e) Technology audit and (f) Internal awareness and training. Meanwhile, the Security Commission Malaysia (SC) has released guidelines on technology risk management. The guidelines incorporate (a) Governance, (b) Technology risk management, (c) Technology operations management, (d) Technology service provider management, (e) Cyber security management and (h) guidance to adopt artificial intelligence (AI) and machine learning (ML).	Technology risk management guidelines	(BNM 2023; SC 2023)
Pakistan (C9)	The State Bank of Pakistan (SBP) produced guidelines on enterprise technology governance & risk management framework for financial institutions. The guidelines incorporate (a) Information technology governance, (b) Information security, (c) IT services delivery & operations management, (d) Acquisition & implementation of IT systems, (e) Business continuity and disaster recovery and (f) IT audit.	Enterprise technology governance & risk management framework guidelines	(SBP 2017)

to be continued …

… continuation

Singapore (C10)	The Monetary Authority of Singapore (MAS) produced guidelines on technology risk management (TRM). The guidelines incorporate (a) Technology risk governance and oversight, (b) Technology risk management framework, (c) IT project management and security-by-design, (d) Software application development and management, (e) IT service management, (f) IT resilience, (g) Access control, (h) Cryptography, (i) Data and infrastructure security, (j) Cyber security operations, (k) Cyber security assessment, (l) Online financial services and (m) IT audit.	Technology risk management guidelines	(MAS 2021)
USA (C11)	The Federal Financial Institutions Examination Council (FFIEC) produced guidelines on information security. The guidelines incorporated (a) Governance of the information security program, (b) Information security program management, (c) Security operations and (d) Information security program effectiveness.	Information Security Guidelines	(FFIEC 2016)

2.4.2 Baseline Policy and Guidelines for Cyber Risk Management

Since this research focuses on financial institutions in Malaysia, the analysis will be focused on the RMiT policy by BNM, as it is a policy that must be complied by all financial institutions in Malaysia. Enforcing measures may be taken if there is non-compliance (BNM 2023). Furthermore, (Marotta & Madnick 2021) highlighted the significance of adhering to current cybersecurity standards in combatting cyber security incidents. TRM by MAS is compulsory for financial institutions in Singapore (Magnus et al. 2019) which is not applicable for Malaysia's financial institution. The same situation is applied to other policy and guidelines from other countries which only applies to their government agencies, critical infrastructure (CSH 2019) or financial institution (Martin 2009; RBI 2011; SBP 2017). Australia's Cyber Security Strategy 2020 is a cybersecurity strategic plan for Australia which centred on the ministry of law enforcement and national security (Uren 2020) and not extensive on cyber risk management.

Several aspects of the cyber risk management framework specified in the RMiT are lacking in cyber awareness and education to the customer and third-party (i.e.

vendor, outsourcing partners) (BNM 2023). Financial institution is required to provide customer care assistance and training in e-banking, online insurance, and online takaful. Still, it does not emphasise on education for cyber security or cyber risk. When a cyber incident occurs, they will impact the stakeholders, including customers and third-party. It is critical for all financial institutions to conduct awareness to bank employees and other stakeholders, including customer and third-party through training and educations (Uddin et al. 2020). Comparison between guidelines by distinct nations on their target audience for awareness and education is referred in Table 2.3.

Table 2.3 Awareness and Education Target Audience in Policy or Guidelines

Country	Reference	Employee	Customer	Vendor	Agent/Partners
Australia	(CISC 2022; DHA 2020)	/	/	x	x
Bangladesh	(BB 2015)	/	/	x	x
Canada	(OSFI 2022a)	/	/	/	/
Europe	(EBA 2019)	/	/	/	x
Group of Seven (G7)	(G7 2016)	/	x	x	x
India	(RBI 2011, 2016)	/	/	/	/ (2016)
Japan	(CSH 2019)	/	x	x	x
Malaysia	(BNM 2023; SC 2023)	/	x	x	/ (SC)
Pakistan	(SBP 2017)	/	/	x	x
Singapore	(MAS 2021)	/	/	/	/
USA	(FFIEC 2016)	/	/	x	x

Based on Table 2.3, Malaysia through BNM RMiT, G7 and Japan have not addressed awareness and education for customer, vendor, and agent/partners. While, Australia, Bangladesh, Canada, Europe, India, Pakistan, Singapore, and USA have addressed it for customer. Canada, Europe, India, and Singapore have also addressed it for vendor. For agent/partner, only Canada, India, Malaysia through SC has addressed it.

Common technology usage (e.g., web and mobile application) and emerging technology such as cloud, IoT, blockchain and ML/AI are also contributing to cyber risks. Application and mobile device technologies are covered by most of the guidelines

except for Bangladesh, Canada and Europe as the guidelines are technology agnostic. However, emerging technology risks are not being addressed consistently in the guidelines. Comparison between guidelines by distinct nations on the coverage of emerging technology are referred in Table 2.4.

Table 2.4 Emerging Technologies in Policy or Guidelines

Country	Reference	Cloud	IoT	Blockchain	ML/AI
Australia	(CISC 2022; DHA 2020)	x	/ (DHA 2020)	x	x
Bangladesh	(BB 2015)	x	x	x	x
Canada	(OSFI 2022a)	x	x	x	x
Europe	(EBA 2019)	x	x	x	x
Group of Seven (G7)	(G7 2016)	x	x	x	x
India	(RBI 2011, 2016)	/ (RBI 2011)	x	x	x
Japan	(CSH 2019)	/	/	x	x
Malaysia	(BNM 2023; SC 2023)	/	x	/ (SC 2023)	/ (SC 2023)
Pakistan	(SBP 2017)	/	x	x	x
Singapore	(MAS 2021)	/	/	x	x
USA	(FFIEC 2016)	/	x	x	x

India, Japan, Malaysia, Pakistan, Singapore, and USA have specified cloud in their guidelines. Australia, Japan, and Singapore have discussed on IoT in the guidelines. Blockchain and ML/AL have been included in Malaysia guideline by Security Commission. For Bangladesh, Canada and Europe, emerging technologies not being discussed specifically because to make certain that the guidelines are independent of technology. G7 guideline is a generic guideline which does not deep dive into emerging technologies.

Based on the analysis, Malaysia through RMiT does not specify cyber awareness and education to the customer and third-party (i.e. vendor, outsourcing partners). It is important to implement controls addressing risk emerged from lack of awareness and education, which is consistent with findings by Foundry where 87% of security leaders admitted that security incidents are caused by non-malicious user error

(34%) (Foundry 2022). In terms of emergence technology, RMiT has only specified cloud technology. IoT, blockchain and ML/AI are not included in RMiT. Typical technology such as web and mobile applications have been addressed in RMiT.

Therefore, based on analysis of available frameworks and guidelines, this research will cover cyber risk controls components which include cyber awareness for customer and third-party and cover technologies such as cloud, web, and mobile application.

2.5 CYBER RISK IDENTIFICATION COMPONENTS

Risk identification comprised of three components; 1) criticality, 2) threat and 3) vulnerability (Bass & Robichaux 2001). It is important to recognize cyber actors, threats and vulnerabilities for cyber risk identification in effectively managing risk (Hoffmann et al. 2020). Figure 2.3 explains the cyber threats and vulnerabilities relationship.

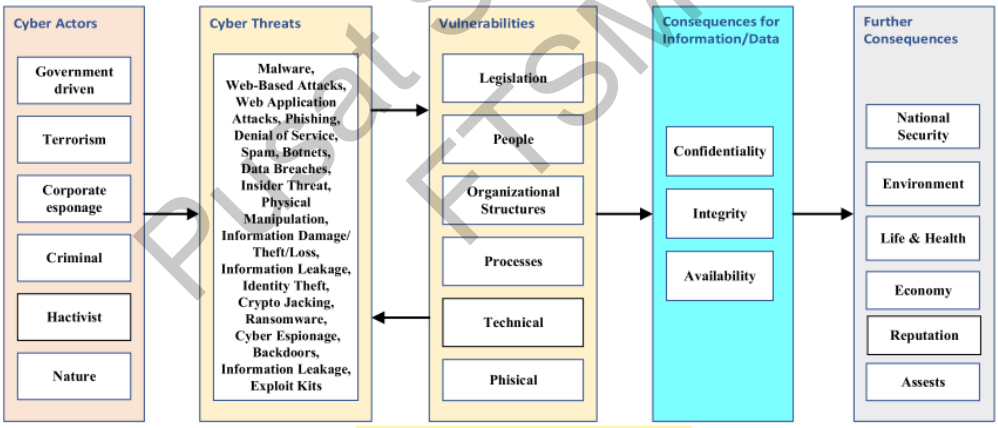

Figure 2.3 Threats and Vulnerabilities Relationship

Source: Hoffmann et al. (2020)

From Figure 2.3, cyber actors are defined as 1) government driven, 2) terrorism, 3) corporate espionage, 4) criminal, 5) hacktivist and 6) nature. Threats are categorized as 1) malware, 2) web-based attack, 3) web application attacks, 4) phishing, 5) denial of service, 6) spam, 7) botnets, 8) data breaches, 9) insider threat, 10) physical manipulation, 11) information damage/theft/loss, 12) information leakage, 13) identity theft, 14) crypto jacking, 15) ransomware, 16) cyber espionage, 17) backdoors and 18)

exploit kits. Vulnerabilities are categorized as 1) legislation, 2) people, 3) organizational structures, 4) processes, 5) technical and 6) physical.

Refsdal et al. (2015) also incorporated threat actor (threat source), threat and vulnerability as part of risk identification components. Additionally, asset and incident components are also included. Figure below showed the risk components resulted from malicious threats.

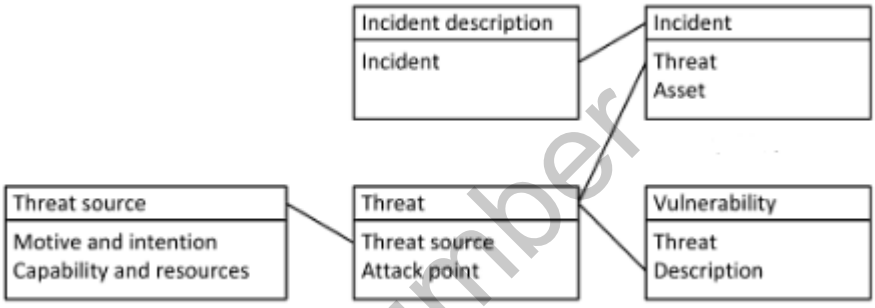

Figure 2.4 Risk Resulted from Malicious Threats
Source: Refsdal et al. (2015)

Criticality refers to how valuable an asset is to the organization. In this study, criticality of assets will be included under Asset, which is one of the components of Cyber Risk Identification framework. Cyber threat actor, threats and vulnerabilities will also be included and discussed.

For cyber risk identification specific to technology such as web and mobile application, OWASP Top 10 Web Application (OWASP 2021) and OWASP Mobile Top 10 (OWASP 2023) described the greatest cyber risks to web applications and mobile application or device. Table 2.5 described the cyber risk for web and mobile application or device.

Table 2.5 Cyber Risk for Web and Mobile Application or Device

Type	Cyber Risk	Reference
Web Application	A01:2021-Broken Access Control A02:2021-Cryptographic Failures A03:2021-Injection A04:2021-Insecure Design A05:2021-Security Misconfiguration A06:2021-Vulnerable and Outdated Components A07:2021-Identification and Authentication Failures A08:2021-Software and Data Integrity Failures A09:2021-Security Logging and Monitoring Failures A10:2021-Server-Side Request Forgery	(OWASP 2021)
Mobile Application or Device	M1: Improper Credential Usage M2: Inadequate Supply Chain Security M3: Insecure Authentication/Authorization M4: Insufficient Input/Output Validation M5: Insecure Communication M6: Inadequate Privacy Controls M7: Insufficient Binary Protections M8: Security Misconfiguration M9: Insecure Data Storage M10: Insufficient Cryptography	(OWASP 2023)

For cyber risk identification specific to cloud technology, according to Cloud and Web Security Challenges in 2022 by Cloud Security Alliance (CSA 2022), organizations are most alarmed with the risks on cloud as specified in Table 2.6.

Table 2.6 Cyber Risk on Cloud

Type	Cyber Risk	Reference
Cloud	Account takeover Authentication abuse Compromised user Denial of service Fraud Loss of system access Persistent adversarial access Privilege user escalation Ransom Sensitive data loss/exfiltration System sabotage	(CSA 2022)

In this study, cyber risk identification specific to technology such as web and mobile application and cloud will be referring to OWASP and CSA.

2.6 INTERNAL DOCUMENT REVIEW

In this section, nine documents from Bank Z have been reviewed which comprise of strategic plan, frameworks, policies, and reports. Relevant information to the research has been extracted and presented in this section.

2.6.1 D1. Cybersecurity Strategic Plan (CSP)

Bank Z has established a cybersecurity strategic plan (CSP) for agility in business growth, facilitate risk management and preserve confidences of its stakeholders. The development of this strategic plan has taken into consideration the bank's internal and external sources to ensure the plan are aligned with business plan, regulatory requirements, and cybersecurity guidelines. Figure 2.5 shows the cybersecurity strategic planning.

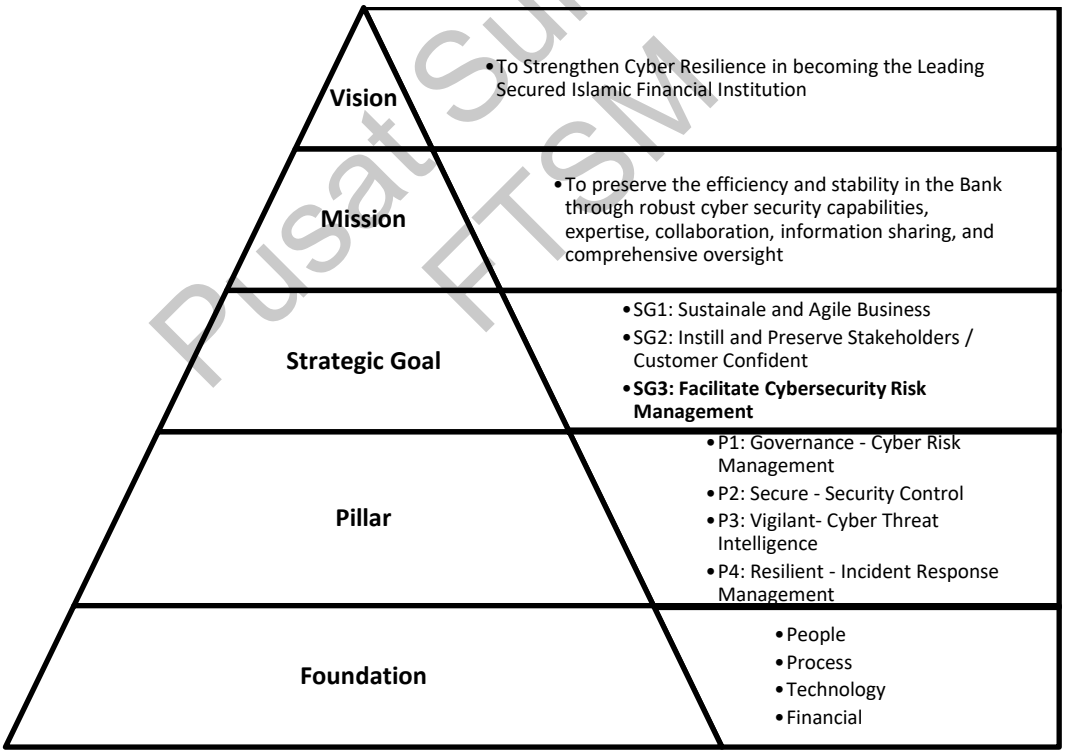

Figure 2.5 Cybersecurity Strategic Plan

Based on the Figure 2.5, the Strategic Goal 3 (SG3) mentions on facilitating the cybersecurity risk management in the bank. This goal is supported by the pillars. Pillar

1 (P1) – Governance emphasizes on ensuring that risks are adequately mitigated, and controls are implemented to mitigate cyber risks. Pillar 2 (P2) – Secure highlights on safeguarding customers information and bank transactions within the bank system infrastructure and application. Pillar 3 (P3) – Vigilant supports on continuously and carefully foresight for possible cybersecurity risk or cyber threat related to the bank. Pillar 4 (P4) – Resilient stresses on the ability to foresee, withstand, bounce back from, and adapt to unfavourable circumstances or compromises on resource-enabled systems.

The CSP also outlines the cyber resilience maturity level that the bank needs to achieve. There are five levels that indicate the Bank's capabilities and standings in terms of cyber security and resilience levels. However, achieving higher levels of maturity doesn't indicate the bank is risk free, rather it allows the bank to further strengthen their security posture and improve their confidence level in terms of cybersecurity and resilience. Refer Figure 2.6 for cyber resilience maturity level.

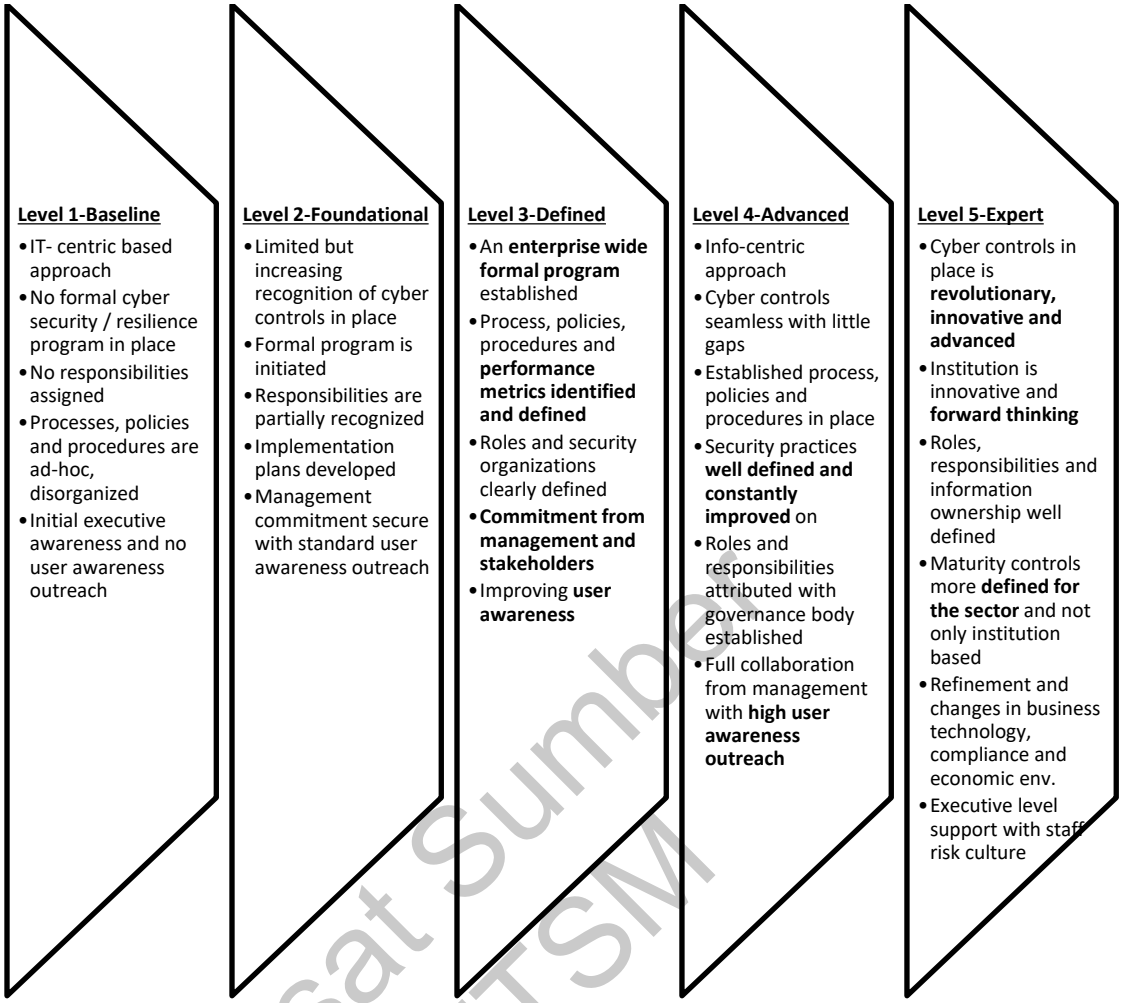

Figure 2.6 Cyber Resilience Maturity Level

In this research, the cybersecurity strategic plan will be part of cyber risk control component to address the cyber risk at the strategic level.

2.6.2 D2. Cyber Resilience Framework (CRF)

The Cyber Resilience Framework (CRF) drives and assists the bank to manage cyber risk effectively and collectively. It is constructed from the four pillars of CSP which are governance, secure, vigilant, and resilient. The pillars are transformed into cyber risk control domains which address people, process, and technology aspects as illustrated in Figure 2.7.

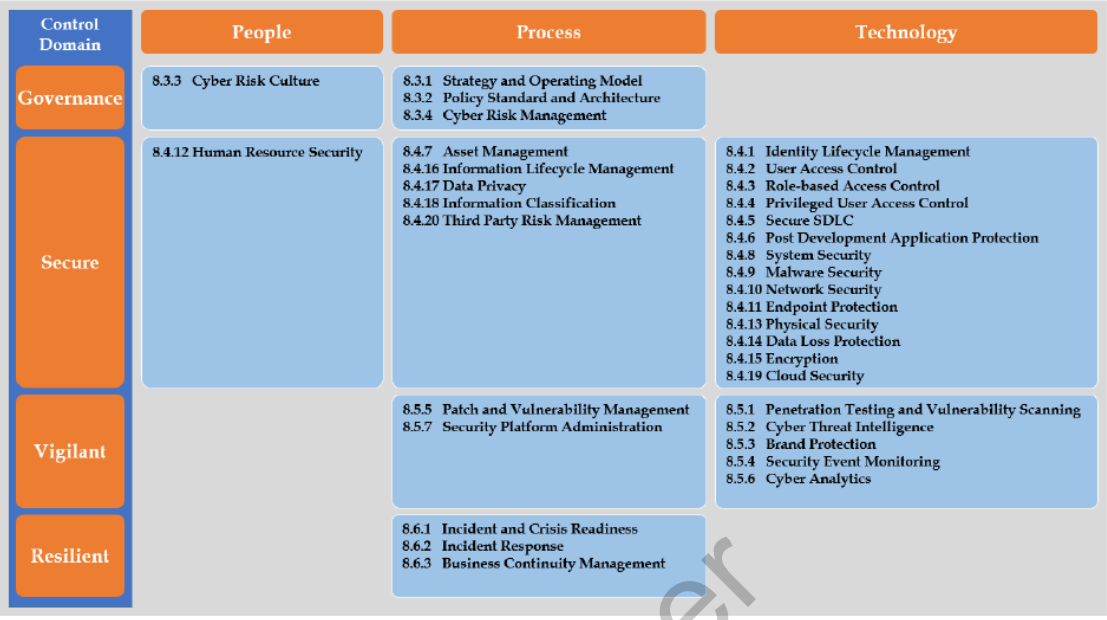

Figure 2.7 Cyber Resilience Framework components

Cyber Risk Control Domain 1: People aspect, 1) cyber risk culture and 2) human resource security is described. Cyber risk culture is depicted on cyber risk training and awareness activities to be conducted periodically at every staff level. However, it does not include third-party and customer.

Cyber Risk Control Domain 2: Process aspect, it consists of 1) strategy and operating model, 2) policy standard and architecture, 3) cyber risk management, 4) asset management, 5) information lifecycle management, 6) data privacy, 7) information classification, 8) third party risk management, 9) patch and vulnerability management, 10) security platform administration, 11) incident and crisis readiness, 12) incident response and 13) business continuity management.

Cyber Risk Control Domain 3: Technology aspect, it consists of 1) identity lifecycle management, 2) user access control, 3) role-based access control, 4) privileged user access control, 5) secure software development life cycle (SDLC), 6) post development application protection, 7) system security, 8) malware security, 9) network security, 10) endpoint protection, 11) physical security, 12) data loss protection, 13) encryption, 14) cloud security, 15) penetration testing and vulnerability scanning, 16)

cyber threat intelligence, 17) brand protection, 18) security event monitoring and 19) cyber analytics.

In this research, the mitigation controls in terms of people, process and technology defined in D2 CRF will be used as cyber risk controls classifications and proactive controls. Cyber risk culture inclusive of staff, third-party and customer under Cyber Risk Control Domain 1: People will also be included in cyber risk proactive controls of the framework.

2.6.3 D3. Technology Risk Management Framework (TRMF)

The Technology Risk Management Framework (TRMF) is devised to support the bank in managing technology and cyber risk effectively. Based on Figure 2.8, the framework comprised of three components: Technology Risk Governance, Business Objective and Technology Risk Element.

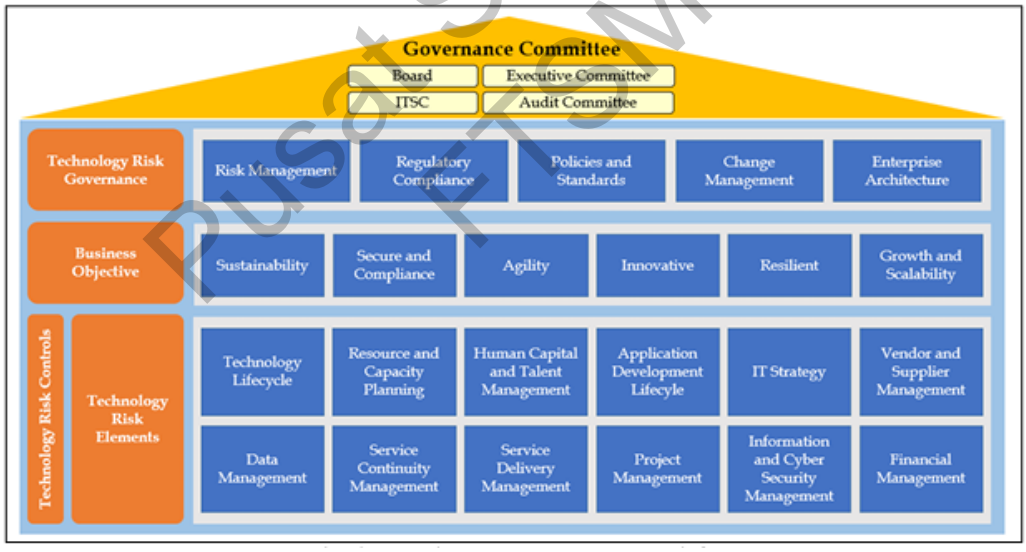

Figure 2.8 Technology Risk Management Framework

Under Technology Risk Governance, it consists of several components which are 1) risk management, 2) regulatory compliance, 3) policies and standards, 4) change management and 5) enterprise architecture.

For Business Objective, it consists of components such as 1) sustainability, 2) secure and compliance, 3) agility, 4) innovative, 5) resilient and 6) growth and scalability.

Under Technology Risk Elements, it consists of 1) technology lifecycle, 2) resource and capacity planning, 3) human capital and talent management, 4) application development lifecycle, 5) IT strategy, 6) vendor and supplier management, 7) data management, 8) service continuity management, 9) service delivery management, 10) project management, 11) information and cyber security management and 12) financial management.

D3 TRMF has defined the mitigation controls such as on applications, third party and related to staff education and awareness. However, it does not cover education and awareness for vendor and customer.

D3 TRMF risk coverage is including non-cyber risk which are related to technology risk which are resource & capacity planning, IT strategy, project management and financial management. This document also does not include cloud in its scope. It also did not specify on threat intelligence as a source of risk identification. The coverage of this document does not comprise of physical and environmental risk.

In this research, cyber risk identification will include components on 1) threat intelligence and 2) categorization of assets. Cyber risk controls will include 1) cyber security education and awareness on staff, third party (i.e vendor, agent) and customer, 2) secure application development lifecycle, 3) vendor supplier agreement, 4) physical and 5) cloud. Future research may cover non-cyber risk which are related to technology risk which are resource & capacity planning, IT strategy, IT project management and financial management and environmental risk.

2.6.4 D4. Cloud Risk Management Framework (CRMF)

The D4 Cloud Risk Management Framework (CRMF) is to drive and support the bank in managing cloud related risk effectively and collectively. It is used to identify,

eliminate, and minimize risks within the cloud environment. D4 CRMF has specified the cyber risk for cloud as following:

1. **Management interface compromise** is a risk where malicious users can impact the entire provisioned cloud infrastructure via the misuse of the management interface.
2. **Resource exhaustion** is a risk whereby the cloud provider is unable to provide the necessary resources needed for clients. This could be due to a variety of factors such as partial failure of the cloud infrastructure due to DDoS attack.
3. **Isolation failure** refers to the risk whereby the isolation controls needed to separate tenant's information and instances fail or are non-existent. This can lead to situations whereby a change in one cloud tenant's instance impact the data or information in another tenant's instance jeopardizing data integrity.
4. **Data mishandling risks** is regarding data mishandling practices by cloud provider which is difficult for cloud user to effectively validate. This occurs when sensitive information is copied, shared, accessed, stolen, or otherwise used by cloud provider's employee who isn't authorized to do so.
5. **Insecure or incomplete data deletion** is when the data is not being wiped properly which resulted in residual data. This scenario may happen during Provider or user exit activity. Because extra copies of the data are stored but not accessible, or because the disc that needs to be destroyed also houses data from other clients, adequate or timely data deletion may also be impossible (or undesirable from the perspective of the customer). Reusing hardware resources and having several tenants provide a bigger risk to the client than dedicated hardware does.
6. **Malicious insider risk** may cause by disgruntled employee, system admin of cloud service provider and managed security service providers which can perform malicious actions in the cloud. The malicious acts can be in the form of unauthorized data access, deletion, and others.

For this research, the cyber risk discussed in D4 CRMF will be included as cyber risk identification components in the proposed framework.

2.6.5 D5. Information Security Policy (ISP)

Policy on Information Security is established to outline the security requirements of an information system. It consists of 1) information asset management, 2) information risk management, 3) human resource security, 4) physical & environmental security, 5) communications and operations management, 6) access control, 7) information system acquisition, development, and maintenance, 8) information security incident management, 9) business continuity management and 10) compliance.

D5 ISP has clearly defined the information assets categorization. It also described the threats and vulnerabilities that which is the basis of identifying cyber risk. All three documents D2 CRF, D3 TRMF and D5 ISP have described similar risk elements on application, third party and staff education which focuses more on controls or mitigation of the risk. D5 ISP and D2 CRF also discussed about cyber threat intelligence as part of risk identification. This policy has also defined the risk assessment process that includes defining information security risk criterion and determination of controls as part of risk treatment plan.

FD5 ISP did not specify penetration testing as part of its control. In terms of technology, D5 ISP did not cover cloud risk, IoT, blockchain and other emerging technology risk. However, it does cover web application and mobile application risk.

For this research, the controls specified in ISP and cloud will be included in cyber risk controls component of the framework. Information assets categorization, threats and vulnerabilities will be part of the cyber risk identification components of the framework. Risk assessment and cyber threat intelligence will be part of reference component of the framework.

2.6.6 D6. Cloud Security Policy (CSP)

Policy on Cloud Security is established to outline the security requirements for the usage of the cloud services prior to the subscription or acquisition of the service itself. The components of cloud security are depicted in Figure 2.9.

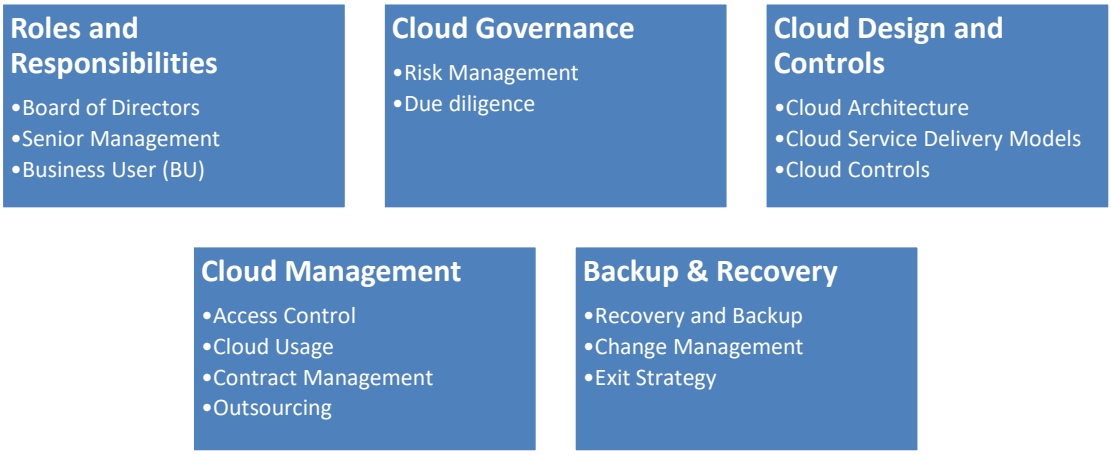

Figure 2.9 Cloud Security Components

It consists of roles and responsibilities for Board of Directors, Senior Management and Business User (BU) in ensuring cloud usage is securely implemented. The policy also emphasized on Cloud Governance which includes risk management which: a) exclusively designed according to the service models being used or considered to use by the Bank; b) clearly define the scope of responsibility for every shared responsibility model. Risk assessment should be conducted on; a) Sophistication of the deployment model; b) cloud infrastructure location; c) Multi-tenancy or data co-mingling; d) Vendor lock-in and application portability or interoperability; e) Ability to modify cloud infrastructure security setups to ensure high levels of data and technology system defence; f) Cyberattacks through cloud service providers; g) The possibility of securing the Bank's data once a cloud service provider is terminated; h) Definition of the service provider's obligations, restrictions, and liability; and i) Ability to consistently adhere to international regulations and cloud computing standards.

For the implementation of critical systems in public cloud, the bank should address the risks in terms of the effectiveness of the overall cloud adoption plan of the bank as following: i) cloud strategy and cloud operational management are overseen by the board.; ii) roles and duties of senior management in cloud management; iii) execution of routine operational management tasks; iv) control and supervision of cloud service providers by the organisation; v) the effectiveness of risk management and internal control procedures; and vi) internal competency and experience fortes.

The bank should also address the risk in terms of accessibility of cloud service providers' independent, accepted globally certifications, at a lowest, in the following areas: i) framework for information security management that uses cryptographic components for user data encryption and decryption; and ii) cloud-specific security controls for protecting client and partner or proprietary information in use, storage, and transit, including payment transaction data.

Cloud configuration should also address: i) geographical duplication; ii) high availability; iii) scalability; iv) portability; v) interoperability; and vi) to protect against probable Internet problems, a solid retrieval and resuming capability is required, as well as an adequate alternate Internet path.

Under Cloud Design and Controls, cloud architecture to adopt 'zero-trust' principle in ensuring enhanced access control for the cloud services. It is also encouraged to use the updated network architecture approach like SD-WAN to manage and monitor granular network security in the cloud network environment. Segregating the network upon leveraging cloud infrastructure is also to be considered.

Data classification should be considered when choosing the cloud service supply models of Software-as-a-service (SaaS), Platform-as-a-service (PaaS) or Infrastructure-as-a-service (IaaS). Cloud controls is to be identified and segregate between critical and noncritical systems in cloud infrastructure.

Cloud Management should consider appropriate control measure upon granting authorisation rights to access the management plane to avoid the risk of cyber-attacks. A complete inventory of bank critical application, system and information assets that is hosted on the cloud need to be clearly defines ownership and updated regularly based on the changes of IT assets and deployment. Under contract management, terms, obligations, responsibilities, liability, and operational standards are to be define in the contract with the cloud provider. Jurisdiction risk should be avoided where local regulatory requirements are complied, local customer protection legislation protect the bank for case of data breach by cloud provider and outsourcing policy are complied in the case of cloud provider services outside the country. Outsourcing partner (i.e fourth

party service) should be informed to the bank and to ensure continuous compliance to policy and regulatory requirements by them.

Recovery and backup need to be tested to ensure no business disruption during operational. It is required to have adequate virtual machine and container backup and recovery, including backup configuration settings (for IaaS and PaaS, as appropriate). Exit plan that clearly defines operational arrangements to facilitate a service provider's exit is required to ensure the bank's continuous operation.

Therefore, this policy has defined the risk identification and mitigation controls for cloud technology which will be included in the framework.

2.6.7 D7. Report of Cyber Incident

a. D7.1 Distributed Denial-of- Service (DDoS)

There has been a reported incident on Distributed Denial-of- Service (DDoS) in November 2022. This incident is categorised as a DNS queries DDoS attack. The DDoS Activity was targeting the bank's online retail banking portal. It was detected by Web Application Firewall (WAF) deployed in the bank. The bank's Security Operation Centre (SOC) has detected a "High Inbound traffic" use case, a "Possible Brute Force" use case, and a "Multiple failed login" detection use case.

The impact of the DDoS attack has exhausted the Java memory which forced the web service to keep on restarting. Thus, the access to retail banking portal was disrupted for more than 7 hours which denied authorized user to access this portal. The attacker did not successfully enter the system.

The mitigation to prevent this DDoS attack was to block the IP addresses detected and revise the threshold setting in WAF to detect DDoS activity with the detected pattern. Additionally, the notification from WAF once an attack is detected need to deliver to SOC Security Information and Event Management (SIEM) for remediation and investigation purpose.

For this research, DDoS attack will be included as cyber risk identification component in the framework. The mitigation controls of DDoS (e.g. WAF, SOC, SIEM) will be included in cyber risk controls component of the framework.

b. D7.2 Disclosure of customer sensitive information to public

In September 2022, an external agent from Bank Z has posted Bank Z's financing letter offer (LO) of three customers on Facebook. The affected customers were not aware that their LO were being posted on Facebook with their personal information on it. In terms of incident handling, it was not clear on department that will need to act on removing the posting from social media.

Identity theft and regulatory fines can occur if sensitive information is disclosed. It may also lead to cybercrime where fraudster may be able to open new accounts, credit cards or financing using the exposed sensitive information.

The mitigation of this incident was CISO office to request the external agent to take down the unauthorized posting from Facebook. The external agent was given awareness on handling customer's information. The bank's Cyber Incident Playbook will also be updated to include incident handling on unauthorised posting in social media by employee or external agent.

For this research, unauthorize disclosure of customer's sensitive information will be included as cyber risk identification component in the framework. The mitigation controls this incident (e.g. awareness to agent, incident handling process update) will be included in cyber risk controls component of the framework.

2.6.8 D8. Report of Internal Audit

a. D8.1 User ID and Password Disclosure

On August 2022, Internal Audit Department (IAD) visited the production datacentre and observed that the servers and network equipment related to card management system (CMS) are hosted in a dedicated server rack. During the visit, IAD team noted

that the vendor has placed a laptop in the rack for accessing the CMS in performing daily operation and configuration tasks instead of using a direct Keyboard, Video, and Mouse (KVM). Upon further checking, IAD team found that the user ID and password were disclosed on the laptop to facilitate daily operation and system configuration between vendor's personnel.

The impact of the disclosure of user ID and password may introduce internal threat where datacentre staff could access and exploit the system illegally in a way to cause damage or steal data. It may also introduce external threat where the laptop has WIFI capabilities to establish Internet connection and this could result to the possibility of hacker penetrating the laptop to exploit the system. Ransomware/malware could also infect the laptop and spread across network if the laptop is connected to a CMS network.

The root cause of this disclosure is due to lack of awareness on the proper safekeeping of ID and Password. Periodic review for onsite inspections was not performed in ensuring datacentre infrastructure admin & management are working as intended.

The mitigation of this disclosure is to immediately remove the exposed password on the laptop placed in CMS server rack located at the datacentre. Additionally, to consider of having a KVM solution instead of a laptop for the operation and management activities. This is to strengthen the internal control capabilities as well as the information security controls in accordance with the Password Policy (as mentioned in Policy on Information Security). It is also recommended for IT Infrastructure Department to carry out onsite inspections periodically to ensure datacentre facilities are maintained in accordance with TIER 3 Datacentre (DC) and Disaster Recovery Centre (DRC) standards.

For this research, unauthorize disclosure of user's credentials will be included as cyber risk identification component in the framework. The mitigation controls for this incident (e.g. tools enhancement, periodic inspections) will be included in cyber risk controls component of the framework.

2.6.9 D9. Report of Cyber Phishing Simulation

As part of Cyber Security Awareness Program, Technology and Cyber Risk Department has performed phishing simulation campaign for the bank employees and its subsidiaries between 15th - 25th December 2022 to determine the level of susceptibility of employees towards generic phishing attacks. The scenarios deployed in this assessment was crafted to mimic actual services and entice employees into clicking the malicious links and disclosing their personal data. The details of phishing scenario are depicted in Table 2.7.

Table 2.7 Phishing Scenario Details

Scenario	The phishing email was disguised as an email from Bank Z to request all employees to update personal information as part of Multi Factor Authentication mechanism. The email was directed to entice the employees to click on the link and enter their personal data. Once their personal data is submitted, employees were notified that their submission was successfully saved, and the application will be redirect to the actual retail banking portal
Target User	Bank Z employees and its subsidiaries
Total Number	2402 users
Assessment Date	15-25 December 2022
Source Email Address	ithelpdesk@bankZ.co
Phishing Domain	http://bankZ.co

Key observations from this exercise are as following:

1. The risk exposure of Bank Z is considered HIGH from 79 out of 2402 employees that falls under the phishing campaign and clicked on the link that was sent to them through the phishing email. The link in the phishing email redirects the target to malicious website to gain information. A link in other phishing email will indirectly download viruses or malware that could compromise the organization device or network.
2. 19 out of 2402 employees submitted their personal information, which could eventually lead to the disclosure of sensitive information that cyber attackers may leverage for further attacks.

3. 17 out of 2402 employees had notified IT Security and/ or IT Helpdesk team on this phishing activity.
4. Despite the obvious fake URL of the domain name: “bankZ.co“, employees who clicked on the link have supplied their personal information. This demonstrates the lack of awareness of the "dos" and "don'ts" while handling phishing emails.

Recommendations for future improvement are as following:

1. Employees are advised to avoid providing any specific or sensitive information on auto replying to emails, because it can lead to targeted attacks. It also makes the target users a high priority for additional attacks. A detailed Out-of-Office auto responder could position the organization’s security at risk.
2. Employees are advised to separate internal autoresponders from external. If there is a need to set autoresponder for external entities, ensure to provide information as little detail as possible.
3. A face-to-face training will be conducted for specific high-risk users (19 staffs) who fell for the phishing campaign.
4. Ongoing cyber security awareness program will be conducted to educate employees on cyber security knowledge.

The phishing campaigns conducted by Bank Z started from September 2021. Four phishing campaigns successfully conducted within 2021 until 2022. Following table showed the comparison of results for all four campaigns:

Table 2.8 Phishing Campaign Result Comparison

	1st Campaign 1st – 7th Sep 2021	2nd Campaign 25thNov – 1st Dec 2021	3rd Campaign 13th - 20th Apr 2022	4th Campaign 15th – 25th Dec 2022
Total number of targets	2199	2133	2208	2402
Total number of users who clicked the link	434	309	177	79
Total number of same users that fell for all campaign (clicked the link)	0	0	0	0
Total number of users who submitted their personal information	321	203	114	19
Total number of same users that fell for all campaign (submitted information)	0	0	0	0

From the table above, it shows a decrease in trend of staff who click the phishing link and submitted their personal information.

For this research, phishing will be included as cyber risk identification component in the framework. The mitigation controls for phishing (e.g. awareness to staff) will be included in cyber risk controls component of the framework.

2.6.10 D10. BNM Notification Letter on Fraud Cases

A notification letter issued by BNM dated June 2022 specified BNM's keeping an eye out for the rise of 24.3% in online and mobile banking-related fraud events between the years of 2020 and 2021. Digital fraud growth has risen by 33.5% on a global scale.

As a result of the foregoing, BNM claims that an examination of loss events reported shows an increase in the number of fraud instances, which is caused by:

1. Phone calls / SMS (i.e disclosure of credentials via SMS One Time Password (OTP)).
2. Installation of malicious application, where fraudsters can harvest stolen credentials from the installation, to commit fraud.
3. Authorized payment scam (i.e Macau Scam, where customers would make multiple payments across banking system under the threats of fraudsters).

Therefore, BNM advised financial institution to implement countermeasures as following:

1. Detecting illicit transfers of funds
2. Enhancing customer awareness
3. Assisting customer in distress
4. Better industry practices (preventing exploitations of vulnerabilities in the e-banking system)

For this research, fraud will be included as cyber risk identification component in the framework. The mitigation controls for fraud (e.g. awareness to customer, protection of e-banking system) will be included in cyber risk controls component of the framework.

2.7 CONCLUSION

Based on NIST Cyber Security Framework, it is crucial to identify security risks as this is a lacking component (Almuhammadi & Alsaleh 2017). Identify the risk identification function is through conducting risk assessment process. Prior to performing risk assessment, risk needs to be identified clearly to address all possible threats and vulnerabilities. Human risk as workers, suppliers and customers are possible threats and vulnerabilities that requires to be attended by providing controls to prevent technological and cyber incidents (Kosub 2015; Uddin et al. 2020). Emergence technology risk is also a risk that needs to be identified and addressed as most current cyber risk management standards are not specifically focusing on emerging technology

risks such as cloud, blockchain, artificial intelligence (AI) and the Internet of Things (IoT)) (Basori & Ariffin 2022; Fischer 2017; Lee 2020). In this research, framework that is developed will incorporate cyber risk identification and cyber risk controls based on analysis conducted on the existing frameworks, guidelines, risk identification components and documentations from Bank Z.

CHAPTER III

METHODOLOGY

3.1 INTRODUCTION

This chapter presents the research approach and methodology, which comprise research design, sample, instrument, data collection protocol and procedure, data analysis and conclusion.

3.2 RESEARCH DESIGN

Since cyber risk is an advanced key component that can negatively influence the reliability of the banks and financial institutions, related roles such as managers, regulators, and international organisations should prioritise the appropriate administration of cyber risk in banking systems (Goodman & Ramer 2007; Kopp et al. 2017). There are two techniques to manage cyber risk: qualitative and quantitative (Lee 2020). The qualitative technique can be based on risk management frameworks and guidelines as in Table 2.1 and Table 2.2. The quantitative technique can be based on a few techniques such as Bayesian decision network (BDN) (Khosravi-Farmad & Ghaemi-Bafghi 2020; Shetty et al. 2018; Zhang & Kelly 2022) and AVARCIBER which elaborate further on certain factors in ISO 27005 (Rea-Guaman et al. 2020).

This research employs a qualitative approach through a single case study. The chosen case study is one of the financial institutions in Malaysia, referred as Bank Z. Bank Z is a small-sized Islamic bank with total assets of more than twenty-five billion ringgit and is one of the seventeen Islamic banks licensed under BNM. The bank operates nationwide with 68 branches in Malaysia. Bank Z is the first Islamic bank in

the world and the first in Southeast Asian region to be recognized as a member of Global Alliance for Banking on Values (GABV) which reflected the bank's desire to become part of values-based banking movement. Bank Z has developed a Cybersecurity Strategic Plan where its vision is to strengthen cyber resilience in becoming the leading secured Islamic financial institution. One of the strategic goals is to facilitate cyber security risk management. The bank has currently undergone a significant structural and process transformation to improve its technology and cyber security resilience. Technology and Cyber Risk Department was established as a second line of defense for the bank, separated from IT Security Department which function as the first line of defense of cyber threats and attacks. The transformation has resulted in a more focused departmental function to address cyber risk and its mitigations.

The researcher selected the respective bank as the source for case study as it: (1) has dedicated cyber risk department that is progressively enhancing cyber risk management and assessment processes, (2) has cyber security expertise with years of experience from multi-industries background, and (3) allowed the researcher undeterred access to relevant documents and expertise for data collection.

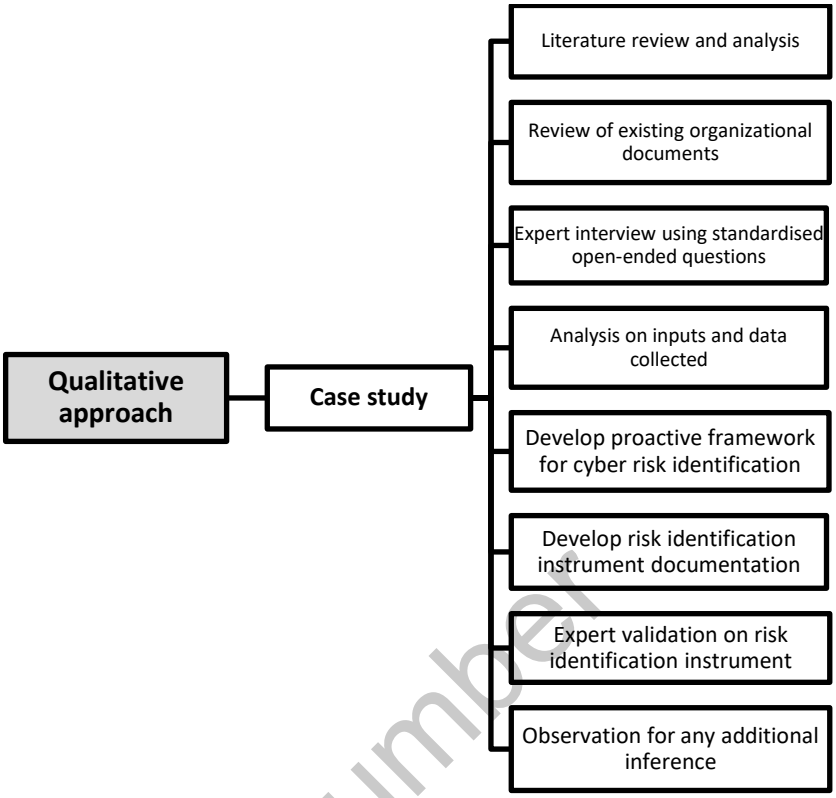

Figure 3.1 Research Design

The research design is shown in Figure 3.1. Based on the research design, literature review and analysis are conducted to identify the components for proactive risk identification framework regarding cyber risk management framework and cyber risk guidelines. A review of existing documents such as organisational cyber security strategic plan, frameworks, policy, reports of cyber incidents, internal audit, cyber simulation activity from Bank Z and circular from regulatory body are performed.

Interviews sessions are conducted using standardised open-ended questions with specialists in the cyber security field who the heads of departments and sections from Bank Z in Malaysia are specialised in cyber security strategic planning, cyber risk, IT security technologies and IT security operations. The questions are related to general cyber security on current threat-landscape in their organisation as financial institution, cyber threats on emerging technologies, cyber risk identification for technology such as banking application, mobile devices and cloud, references for risk identification and cyber risk controls in terms proactive and reactive techniques, challenges to implement

controls and recommendation to address the challenges. The type of questions asked was based on experts' knowledge, experience, and opinion.

Based on the analysis of inputs and data collected, a proactive framework for cyber risk identification management is developed and presented in a risk identification instrument document. The risk identification instrument is reviewed and validated by experts in cyber security domain who are seniors and specialists from Bank Z to ensure it meets the research objectives.

Observations are performed to find any additional inference based on research approaches that have been conducted.

3.3 RESEARCH METHOD: SINGLE CASE STUDY

In this research, data were collected from Bank Z in Malaysia. The target sampling were two departments in Bank Z: Technology and Cyber Risk Department and IT Security Department. The following Table 3.1 shows the research instruments involving the experts, department, designation, roles and quantity. An explanation of research instruments is described in Chapter 3.4:

Table 3.1 Details on Panel of Experts

Research Instrument	Department	Designation	Roles	Quantity
Interview with Experts	Technology and Cyber Risk Department	Chief Information Security Officer (CISO)	Technology and cyber risk & operation strategies, policy formulation, monitoring	1
	Technology and Cyber Risk Department	Head, Cyber Risk	Cyber risk assessment, reporting and monitoring	1
	IT Security Department	Head, IT Security	IT security operation and monitoring strategies, guideline formulation	1
Expert Validation	Technology and Cyber Risk Department	Specialist @ Manager, Technology Risk	Technology risk assessment, reporting and monitoring	1

to be continued …

… continuation

	IT Security Department	Specialist @ Manager, IT Security	IT security operations and monitoring	1
	Total Numbers of Experts			**5**

All the panel of experts are considered experts in cyber security domain with more than fourteen years of experience in cyber security domain ranging from cyber security strategic planning, cyber risk management, IT security technology, IT product security evaluation, information security management system, security audit and IT product security certification. Their working experiences ranged from cyber security agencies in Malaysia and Qatar, more than two financial institutions, multinational manufacturing companies, and multinational and local software development companies in Malaysia. Therefore, the chosen experts are qualified professionals, with years of experience in multi-industries, who offer the most valuable opinions and views on cyber security.

The sampling method chosen was based on the purposive sampling technique. According to Dudovskiy (2022), purposive sampling is a sampling approach in which reasoning are applies to gather members of the populace to participate in the research. It is also indicated to as judgement, selective, or subjective sampling. It is a non-probability sampling method where sample items are chosen based on the researcher's assessment (Black 2019). Because of the nature of the research design and its aims, only a small number of people can serve as primary data sources. This is when the purposive sampling method may be useful (Dudovskiy 2022). One of the categories of purposive sampling is homogeneous sampling. It focuses on a one smaller group in which entire sample members share characteristics, such as an organisation's peculiar profession or level of hierarchy (Saunders et al., 2023).

In this research, all the experts are in cyber security occupations and at least at the managerial level, with vast experience in the cyber security domain.

3.4 RESEARCH INSTRUMENT

There are four instruments used to conduct this research. The instruments are expert interview, document review, expert validation, and observation.

3.4.1 Document Review

Selections of the document were based on documents obtained and accessible from experts in Bank Z. Additionally, the researcher is also part of the personnel working in Bank Z, which has eased the process of obtaining the documentations access. The documents accessible to the researcher comprised of the following:

D1. Cybersecurity Strategic Plan
D2. Cyber Resilience Framework
D3. Technology Risk Management Framework
D4. Cloud Risk Management Framework
D5. Information Security Policy
D6. Cloud Security Policy
D7. Report of Cyber Incident
D8. Report of Internal Audit
D9. Report of Cyber Phishing Simulation
D10. BNM Notification Letter on Fraud Cases

All the documents were non-public documents, and the content was confidential. Therefore, this project could not include all the documents as an appendix. However, the documents' names were used as a reference for the research analysis and discussion purposes.

The documents on strategic planning for cyber security, risk management, cyber risk identification components, methods, references, and control mechanisms were reviewed. Risk framework and security policy on emerging technology used, such as cloud, were also analysed. Finally, analysis was also performed on the previous cyber incident recorded, internal audit findings regarding any non-conformance to security

controls outlined in organisational policy, the outcome of the cyber phishing simulation exercise conducted to staff in Bank Z and circular issued by the regulatory body on an increase of fraud cases. The collected data were examined to discover relationships and concluded in response to the research questions. Inferences were also made based on the collected data.

3.4.2 Interview with Experts

In supporting the data collected from case study approach, data from experts were also being analysed through interview questions. The purpose of this interview is to collect empirical data for proactive framework development. Experts from cyber security strategic planning, cyber risk and IT security technology have been identified to obtain their view from interview sessions. Table 3.2 shows the interview questions that have been shared to the experts. Refer Appendix A for e-mail requesting permission for interview with experts and Appendix B on questions for interview with experts.

Table 3.2 Interview Questions

Section	Category		Question	Reference
A	General	Q1.	Can you share the cyber-threat landscape within your organisation as a financial institution?	(FS-ISAC 2022)
		Q2.	Do you see any trends in cyber threats and attacks focusing on your organisation or the financial institution specifically?	
		Q3.	In your opinion, are there any specific cyber threats on financial institutions that may differ from any other industries?	
		Q4.	Does your organisation implement emerging technologies such as cloud, blockchain or IoT? If yes, please specify which technology.	(Ker 2022; McShane et al. 2021)
		Q5.	How does your organisation perceive the cyber threats on emerging technologies such as cloud?	
		Q6.	How does your organisation manage cyber threats in terms of strategic plan and operations?	
B	Cyber Risk Identification	Q1.	What is the category of assets in your organisation that needs to be protected from cyber threats?	(Von Solms & Van Niekerk 2013)
		Q2.	How does your organisation identify cyber risk?	

to be continued …

… continuation

		Q3.	What is the cyber risk categorisation in your organisation?	(Bass & Robichaux 2001; BNM 2023; CSA 2022; OWASP 2021; OWASP 2023)
		Q4.	In your opinion, what is the cyber risk for technology used in your organisation such as internet banking application, mobile devices and cloud?	
		Q5.	What is the source of reference for your risk identification? Is it according to regulatory body requirements, international standards or best practices? Please highlight the reference.	
		Q6.	In your opinion, does the source of reference being used identify cyber risk from customer, third-party and emerging technologies such as cloud, blockchain and IoT?	
C	Cyber Risk Control	Q1.	How does your organisation identify cyber risk or security control?	(Agamba & Keegnwe 2012; H. Saini 2016; Miller 2016; Y. Chen et al. 2018)
		Q2.	How does your organisation implement proactive and reactive cyber security techniques as part of security controls?	
		Q3.	In your opinion, does implementing proactive cyber security techniques more satisfactory to effectively addressing cyber risk?	(EY 2014)
		Q4.	What is the source of reference for your cyber risk controls? Is it according to regulatory body requirements, international standards or best practices? Please highlight the reference.	(Bass & Robichaux 2001; BNM 2023; CSA 2022; OWASP 2021; OWASP 2023)
		Q5.	In your opinion, does the source of reference being used determine cyber risk controls on cyber security education/awareness for customer and third-party and emerging technologies such as cloud, blockchain and IoT?	
		Q6.	What are the challenges to implement cyber risk controls in your organisation?	(Foundry 2022; Tse 2022)
		Q7.	What is your recommendation to address the challenges in implementing cyber risk controls in your organisation?	

The interview protocol is adapted from Jacob & Furgerson (2012) as follows:

1. Open-ended interview questions are developed to allow greater time and room for the experts to be more forthcoming and detailed in sharing their experiences. Three interviews have been conducted where each session lasted for one hour. In total, three hours have been used to conduct the interviews. Limited sessions of interview conducted due to tight working schedule of experts.

2. Interview questions are based on literature review as in reference from Table 3.2 which ensure the questions are structured based on earlier research that may resulted in similar or different answer. It also will create in a manner that will produce more insightful data from the experts.

3. Interview started with basic questions such as background and experience of the experts as a warming up. It is important to build trust with the experts, so they are comfortable to share valuable data for the research.

4. Interview questions are arranged from high level questions to more in-depth on the research topics. The purpose of it is to gain trust from the experts to answer questions comfortably.

5. Prompts or stimuli experts with points which originate from the literature that will enrich the data or obtain unexpected data. This is also useful to ensure that the experts have not missed to mention any specific points.

3.4.3 Expert Validation

Experts have been asked to validate the developed proactive framework for cyber risk identification and risk identification instrument to ensure it meets the research objectives. Feedback from the experts has been used to improve and update the framework and risk identification instrument.

The proactive framework for cyber risk identification and risk identification instrument have been shared with two experts. Experts have been asked to validate the proactive framework and instrument based on criteria as following: (a) purpose of framework; (b) components of framework and (c) overall impression of the framework. The feedback collected from experts based on these criteria will be analysed and interpreted to improve the proactive framework and instrument for cyber risk identification.

3.5 DATA COLLECTION PROCESS AND PROCEDURE

In this research, the data collection process has been split into two phases. Phase one implicated the initial preparation process in determining the interview questions and

identifying the panel of experts for interview session. In phase two, the research was executed, including interview sessions with experts and document review.

In phase one, prior to interview sessions, interview questions were developed based on literature review and analysis. Then, three experts were identified from Bank Z for interview sessions. Email to request permission for interview session were sent to all experts along with interview questions as reference. Researcher was also one of the staff from Bank Z. Therefore, it was not required to present supporting letter to Bank Z for conducting research and using the Bank's Z data as long that it remained solely for the research purpose. However, the research output may be used to improve the cyber risk identification process in Bank Z to enhance its cyber resiliency.

In phase two, once expert permission was obtained, interview sessions were scheduled and conducted through physical or online meeting using Microsoft Teams. Documentations such as framework, policy and reports from Bank Z shared by the experts were also discussed during interview sessions. All data from interview sessions and documentations from Bank Z were collected for analysis process. Refer to Figure 3.2 for the flowchart of the process and procedure used in this research.

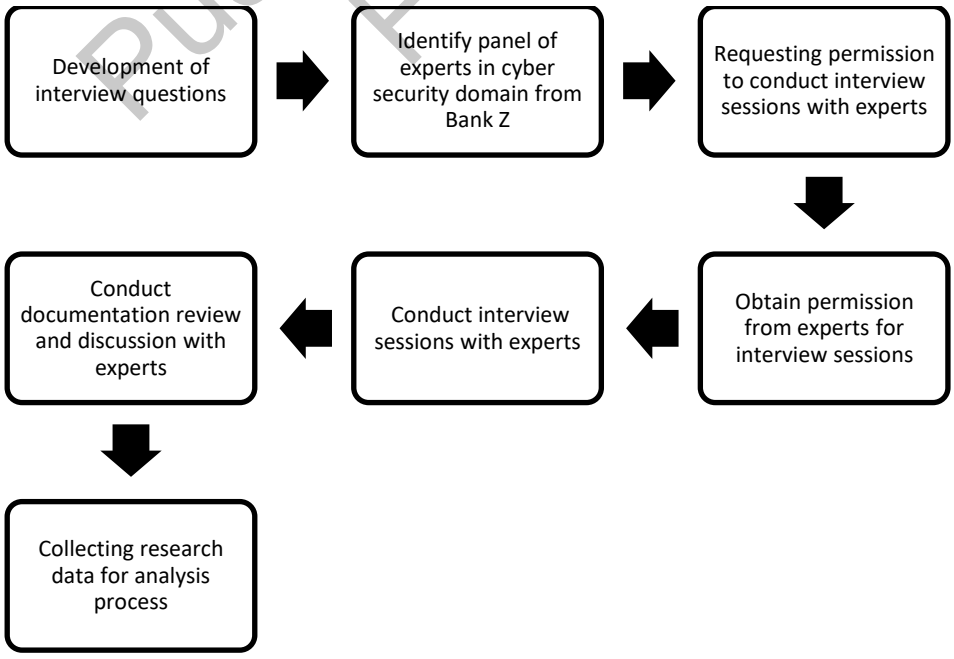

Figure 3.2 Data Collection Procedure

3.6 DATA ANALYSIS

3.6.1 Data Analysis and Interpretation for Qualitative Method

Data preparation for analysis process were obtained from the qualitative method which focuses on documentation review and expert interviews. Data obtained from documentation review and interview sessions were transcribed in Microsoft Word. For online interview session, it was recorded using Microsoft Teams and transcribe in Microsoft Word. The data were manually analysed and transformed into risk identification instrument in Microsoft Excel. All data collected have been documented and analysed to find pattern or trends of cyber threats and attacks, cyber risk identification components and cyber risk controls that focus on financial institution, which fulfill the research objectives and answered the research questions.

For documentation review and analysis, thematic analysis method is used where qualitative data being identified, analyzed and recurring meanings compiled (or "themes"). This method introduce a systematic style to see and process qualitative data using “coding” (Braun & Clarke 2006). The thematic analysis has been conducted in phases according to Braun & Clarke (2006) as following:

1. Phase 1: Data familiarization – Documents were read, and notes were taken on highlights for the respective topic.
2. Phase 2: Generate primary code – Keywords or codes on certain concepts were transcribed to look for commonality in the next phase.
3. Phase 3: Look out for themes – Codes were grouped into possible subjects and all information pertinent to each possible subject were assembled.
4. Phase 4: Review themes – Documents were re-read to confirm the codes and themes. Final themes were decided for analysis which reflected the concept for the group of codes.
5. Phase 5: Define and give the theme a name - Themes were given name according to specific concept. The themes produced were related to research questions. The documents were then analyzed according to these themes.

6. Phase 6: Produce report – After all documents available being analyzed in detail, the interpretation of the data was written according to themes. The interpretations were used to identify the cyber risk components.

The targeted sample data were from ten documentations review. From document review on D1 CSP, the document was analysed to determine whether it outline the strategy for cyber risk management in terms of risk identification and mitigation controls. For D2 CRF, D3 TRMF and D4 CRMF on framework, the documents were examined to verify whether it define the frameworks for cyber risk management related to risk identification and mitigation controls. For D5 ISP and D6 CSP, the documents were explored on risk identification and mitigation controls for technology such as banking application, mobile device, and cloud. For D7, D8, D9 and D10 on reports, the documents were investigated to find the root cause of incident, audit findings, phishing simulation exercise for internal staff and whether it can be related to the absence of controls or ineffective controls by Bank Z and circular by BNM regarding the increase of fraud cases in financial institution.

For expert interview, the targeted sample data were from three expert interview with nineteen questions. From expert interview on Section A. General Questions, the data were analysed to find patterns on cyber-threat landscape for Bank Z or financial institution, trends in cyber threats and attacks focusing on financial institution, specific cyber threats on financial institution, cyber threats on emerging technologies such as cloud and cyber risk management in terms of strategic plan and operations.

For Section B. Cyber Risk Identification Questions, the data were examined to identify assets being monitored from cyber threats, process of cyber risk identification, cyber risk categorisation, cyber risk on common technology used such as banking applications, mobile devices and also emerging technology such as cloud, reference used to identify risk and whether the reference used has included cyber risk from customer, third-party and emerging technologies such as cloud, blockchain and IoT.

For Section C. Cyber Risk Control Questions, the data were scrutinised to identify cyber security controls, implementation of controls in terms of proactive and

reactive perspectives, effectiveness of either proactive or reactive controls, reference used to identify cyber risk controls and whether the reference incorporated controls on cyber security education/awareness for customer and third-party and emerging technologies such as cloud, blockchain and IoT. Additionally, challenges to implementing cyber risk controls and recommendations to overcome the challenges were also noted to develop a practical and usable framework.

The analysis of all data was used to recognise the components required for the development of proactive framework for cyber risk identification and risk identification instrument.

3.6.2 Data Validation for Qualitative Method

All data collected were edited regarding grammatical errors or unintended mistakes from the experts. In case of uncertainty of the accuracy of the collected data, researcher has re-visit the interview notes or voice recording of interviews to verify the data. Additionally, two experts which were not part of the interview sessions validated the proactive framework for cyber risk identification management and risk identification instrument. The proactive framework and risk identification instrument have been updated and improved using the experts' feedback.

3.7 CONCLUSION

This research was conducted using qualitative method. The case study approach consists of literature review and analysis, document review, interview with experts, expert validation, and observation. Data were collected from Bank Z in Malaysia. All collected data were analysed using thematic analysis and validated to identify the components to develop the proactive framework for cyber risk identification management and cyber risk identification instrument. The selection of qualitative method for this research is helpful to fulfil the research objectives and solving the research questions.

CHAPTER IV

RESULTS AND DISCUSSION

4.1 INTRODUCTION

This chapter presents the results of the research through data collection activities. Discussion on cyber risk in financial institutions is explained in terms of issues, risk and impact based on literature review and analysis activities. Documentation review and expert interview results are analysed and discussed in terms of cyber risk identification and controls, which contribute to developing the proactive framework for cyber risk identification (PROCRIF). Finally, the conclusion of the results is described as an overall analysis of the research.

4.2 CYBER RISK IN FINANCIAL INSTITUTION

4.2.1 Issues, Risk, and Impact

Based on the annual report of cyber risk and forecasts for 2022 (FS-ISAC 2022) specific to the banking sector, the highest exploitation are zero-day vulnerabilities, third-party or service provider attacks, ransomware, social engineering, fraud and DDoS. The forecast is supported by the Data Breach Investigation Report 2022 (Gabriel Bassett, C. David Hylender, Philippe Langlois, A.Pinto 2022) where 82% of breaches are related to an individual factor from phishing activity. It also highlighted that ransomware incident makes up 25% of total breaches. Also, the supply chain or third party makes up 62% of system intrusion incidents.

Cyber risk in financial institutions is aligned with the cyber incidents in the global industries. According to the International Monetary Fund (IMF) (Bouveret 2018), the financial sector is experiencing business disturbances due to DDoS attacks

on critical servers. E-banking networks are susceptible to various online dangers, including DDoS attacks. (Abdulla & Al-Hassani 2022). The banking system may be fully taken down by DDoS attacks, which allow attackers to install malware or other spyware (Beitollahi & Deconinck 2012; Uddin et al. 2020). An example of the incident is a DDoS attack launched on 8th July 2014 on seven major financial institutions in Norway that resulted in service disturbance for the whole day (Bouveret 2018).

Data breaches are also susceptible to the financial sector, where this sector has experienced most data loss instances. Internal systems are hacked, which results in data breaches (Catota et al. 2018; Glazer 2014). An example of the incident is the Equifax data breach, where over 145 million US consumers' personal information may have been stolen by attackers (Bouveret 2018). A Moroccan bank experienced a breach of consumer accounts and transactions without authorisation in August 2020. (Popović 2021).

Fraud is also mentioned in (Bouveret 2018), where cyber-criminals may access client login information for online payments and use those credentials to access financial institution systems. A classic example was the SWIFT attacks from 2015 until 2018, which resulted in USD 336 million in losses. Typically, this kind of attack is originated from a successful phishing activity. (Aldasoro et al. 2022) also supporting the fact that the financial sector experiences the highest number of cyber incidents, including data loss. Looking at the Malaysian perspective, cyber incident statistics by CyberSecurity Malaysia ranging from January to September for the year 2022 (MyCERT 2022) show among the highest cases is fraud with 3992 cases, which is aligned with the other findings.

It is also worth mentioning that technological advancements or emerging technologies such as cloud, blockchain, artificial intelligence (AI) and Internet of Things (IoT) may make an organisation more susceptible to cyber-attacks. This is due to more attack surfaces created by these technologies that may enable attackers to try and penetrate the targeted financial system (Bouveret 2018). Cyber security threats will proliferate due to organisations' increased reliance on modern technology, such as AI and system interconnectedness, such as blockchain, cloud computing, and IoT

(McShane et al. 2021). There is a need to address cyber risk in applications that use emerging technologies being developed and improved to make them more secure (Ker 2022) as following:

1. For the cloud the wider use of cloud services exposes the financial sector to cyber-attack cases (Aldasoro et al. 2022). (Alani 2016) stated the threats in cloud computing are data breaches, data loss, hijacking of accounts and cloud services and use of insecure APIs. (CSA 2022) has also listed the main threats to cloud computing. Among them are lateral movements using affected accounts to send internal phishing, command and control through non-standard ports, access credentials obtained from websites, and privilege escalation.
2. For blockchain, the cyber security risk is to maintain the consistency and reliability of the data to maintain the integrity of the data. Only authorised bank employees can alter kept data (Ali et al., 2018). Blockchain verification technology must be safeguarded to stop hackers from manipulating and gaining access to the blockchain network if used in the financial sector (Basori & Ariffin, 2022).
3. For artificial intelligence (artificial intelligence) / machine learning (machine learning), there are also cyber threats, such as manipulating data at the AI/ML life cycle stage. These threats can cause systems based on AI/ML to make wrong decisions or extract sensitive information (Vučinić & Luburić 2022).
4. For IoT, vulnerabilities and threats can come from application, processing, network, and perception layers, such as attackers gaining access and modifying unencrypted data packets in transmission. Digital Lighting Management (DLM) sensors can be used in DDoS attacks (Lee 2020).

The reliance on third parties, where businesses outsource tasks to a few specialised suppliers, could affect the financial system when being attacked (Bouveret 2018; Eisenbach et al. 2022). With the higher adoption of the cloud, financial institutions rely on third-party cloud security providers (CSP) to store, transfer, and process data, which may lead to attacks in the multi-tenant environment (Peihani 2022). Due to the provider's importance to the financial system, the interruption of a provider

in this situation possibly will raise systemic risk that interrupts or collapses the whole financial system (FSB 2017; Peihani 2022).

For the framework development, DDoS, data breach, fraud and third-party risk contribute to the risk identification component of the framework.

For the cloud specifically, data breach, data loss, hijacking of accounts and cloud services, use of insecure APIs, lateral movements using affected accounts to send internal phishing, command and control through non-standard ports, access credentials obtained from websites and privilege escalation contribute to the Risk Identification component of the framework.

4.3 DOCUMENT REVIEW ANALYSIS

The thematic analysis method is used to review the documents. The details of the method have been explained in Chapter 3. Codes and themes produced by performing the thematic analysis method are presented in Table 4.1. Documentations that have been reviewed and analyzed according to the themes are referred to in Table 4.2.

Table 4.1 Codes and Themes from Thematic Analysis

Purpose	Codes		Potential Themes	Final Themes
Identify cyber risk identification	Cyber Risk Identification	i.	Category of assets in an organization that needs to be protected from cyber threats.	CRI.T1.Assets
		ii.	Identify cyber risk in organization.	CRI.T2.Risk Identification & Categorization
		iii.	Cyber risk categorization in organization.	
		iv.	Cyber risk for technology used in an organisation such as internet banking application, mobile devices and cloud	CRI.T3.Technology

to be continued …

… continuation

		v.	Source of reference for risk identification such as regulatory body requirements, international standards or best practices.	CRI.T4.Risk Identification Reference
		vi.	Cyber risk from customer, third-party and emerging technologies such as cloud, blockchain and IoT perspective in source of reference.	
Identify cyber risk control	Cyber Risk Control	i.	Identify cyber risk or security control in an organisation.	CRC.T1. Risk Control Classification
		ii.	Implementation of proactive and reactive cyber security techniques as part of security controls in an organization.	CRC.T2. Proactive Controls
		iii.	Implementing proactive cyber security techniques is more satisfactory to effectively addressing cyber risk.	
		iv.	Source of reference for cyber risk controls such as regulatory body requirements, international standards or best practices.	CRC.T3. Risk Control Reference
		v.	Cyber risk controls on cyber security education/awareness for customer and third-party and emerging technologies such as cloud, blockchain and IoT in source of reference.	
		vi.	Challenges to implement cyber risk controls in an organization.	CRC.T4. Challenges & recommendations
		vii.	Recommendations to address the challenges in implementing cyber risk controls in an organization.	

to be continued …

… continuation

General knowledge on current cyber threat landscape	General	i.	Cyber-threat landscape within an organisation as a financial institution.	G.T1. Cyber threat landscape & trends
		ii.	Trends in cyber threats and attacks focusing financial institution.	
		iii.	Specific cyber threats on financial institutions that may differ from any other industries.	
		iv.	Cyber threats on emerging technologies such as cloud.	
		v.	Managing cyber threats in terms of strategic plan and operations	G.T2. Strategic plan and operation

Table 4.2 Documents Reviewed and Analyzed by Themes

Document	Cyber Risk Identification (CRI)				Cyber Risk Control (CRC)				General (G)		Summary of Content
	T 1	T 2	T 3	T 4	T 1	T 2	T 3	T 4	T1	T2	
D1	x	x	x	x	x	x	/	x	x	/	CSP has defined the facilitation of cybersecurity risk management in the bank. The strategies highlighted are on risk mitigation, implementation of controls to mitigate cyber risks, protection of customer information and bank transaction, continuous monitoring on cyber threat/risk and cyber resilience in anticipate, withstand, recover from cyber-attack. It also discussed on cyber resilience maturity level to measure the bank's security posture.
D2	x	/	/	/	/	/	/	x	x	x	CRF described the controls in terms of people, process, and technology. It discussed about controls on people (training, awareness, governing human resources), process (compliance, reporting, asset management, third party management) and technology (SSDLC, penetration testing, access control, web application, mobile application, cloud).
D3	x	/	x	/	/	/	/	x	x	x	TRMF described the risk identification and mitigation controls on applications, third party and related to staff education and awareness. It also segregates responsibilities between first, second and third line of defense in implementing, reviewing and assurance verification on controls taken.
D4	x	x	/	x	x	/	x	x	/	x	CRMF discussed the framework for risk identification and mitigation controls for cloud technology.
D5	/	/	x	/	x	/	x	x	x	x	ISP defined the risk assessment process that includes defining information security risk criterion and determination of controls as part of risk treatment plan
D6	x	x	/	x	/	/	x	x	/	x	CSP defined the risk identification and mitigation controls for cloud technology.
D7.1	x	/	x	x	/	x	x	x	/	x	Incident report discussed on DNS DDoS attack on the bank's online retail banking portal.
D7.2	x	/	x	x	/	x	x	x	x	x	Incident report discussed on disclosure of customer sensitive information to public using social media.
D8.1	x	/	x	x	/	x	x	x	/	x	Internal audit report discussed on user ID and password disclosure on laptop in datacenter by third party (outsourcing partner).
D9	x	/	x	x	/	x	x	x	/	x	Report on cyber phishing simulation conducted to staff in the bank
D10	x	/	x	x	/	x	/	x	/	x	Notification letter by BNM on the increased of fraud cases among banking customers

Table 4.1 and Table 4.2 contributes to the development of risk identification component and risk control component of the framework.

4.3.1 Cyber Risk Identification (CRI)

Documents being analysed discussed on assets, risk categorization, technology, and reference.

a. CRI.T1: Assets

D5 ISP has clearly defined the information assets which includes database, system records, data files, user guidance, training resources, working procedure, continuity plan and fall-back arrangement. The information assets definition contributes to the development of assets component in the framework.

b. CRI.T2: Risk Identification & Categorization

D2 CRF, D3 TRMF and D5 ISP discussed about risk on application, third party and insider threat which is staff. D2 CRF and D5 ISP also discussed on cyber threat intelligence input. D4 discussed about risk for cloud. All the risk contributes to risk identification component in the framework.

Incidents reported in D7.1, D7.2, D8.1, D9 and D10 which are DDoS, disclosure of customer sensitive information by agent, user ID and password disclosure by vendor, phishing and fraud contributing to risk identification component in the framework. Incidents need to be included as risk identification to ensure the incidents will not be repetitive. The threat actor of the incidents needs to be identified as part of the component in the framework. They are: 1) external attacker (DDoS, phishing, and fraud threat actor), agent (disclosure sensitive information threat actor) and vendor (user ID and password disclosure threat actor).

D2 CRF, D3 TRMF and D5 ISP have discussed on risk category. The Table 4.3 showed the similarities and differences of risk categorization for the three documents.

Table 4.3 Risk Categorization

Risk Category	Document Name			
	D2 CRF	D3 TRMF	D5 ISP	Report & Circular (D7.1, D7.2, D8.1, D9 & D10)
1.Phishing	x	x	x	/
2.Fraud	x	x	/	/
3.Disclosure of customer info	x	x	x	/
4.Disclosure of user ID & password	x	x	x	/
5.Unauthorized access (physical/logical)	x	/	/	x
6.Disruption of processing	x	x	x	x
7.Port-scans attack	x	x	/	x
8.Unauthorized access to privileged accounts	x	x	/	x
9.DDoS	x	x	x	/
10.Anomalous occurrences on host	x	x	/	x
11.Information unauthorized modification and disclosure at rest, in transit and in use	x	x	/	x
12.Information loss, damage, theft and misuse	x	x	/	x
13.System failures	x	x	/	x
14.Dumpster diving	x	x	/	x
15.Unauthorized interception signal for wireless	x	x	/	x
16.Advanced Persistent Threat (APT)	x	x	/	x
17.Data leakage	x	x	/	x
18.Malware attack	x	x	/	x
19.Covert channels and trojan	x	x	/	x
20.Unauthorized software installation	x	x	/	x

The risk categorization from Table 4.3 contributes to the development of risk identification component in the framework.

c. CRI.T3: Technology

D2 CRF, D3 TRMF and D5 ISP have discussed on web and mobile application. Cloud technology risk identification have been specified in D4 CRMF and translated into policy in D6 CSP. However, for other technology such as blockchain, AI/ML and IoT, their risk identification is not specified in any documents. The web application, mobile application and cloud contributes to the development of technology component in the framework.

d. CRI.T4: Risk Identification Reference

Reference component for proactive framework is based on regulatory bodies documents from BNM and SC. Table 4.4 presented the reference documents.

Table 4.4 Reference Documents

Reference Documents	Document Name				
	D2 CRF	D3 TRMF	D4 CRMF	D5 ISP	D6 CSP
1. Risk Management in Technology (RMiT) by BNM	/	/	/	/	/
2.Cyber Resilience for Participants of PayNet's Services by PayNet	/	x	x	/	/
3. Management of Customer Information and Permitted Disclosures by BNM	x	x	x	/	/
4. Guidelines on Technology Risk Management by SC	x	x	x	/	/

All documents are developed based on RMiT by BNM as RMiT is a policy that needs to be complied by all financial institutions. For D2 CRF, it also refers to Cyber Resilience for Participants of PayNet's Services. D5 ISP and D6 CSP are referring to Cyber Resilience for Participants of PayNet's Services, Management of Customer Information and Permitted Disclosures and Guidelines on Technology Risk Management. The regulatory body documents aid to the creation of reference component in the framework. In overall, Table 4.4 contributes to the development of reference component of the framework.

4.3.2 Cyber Risk Control (CRC)

Documents being analysed discussed on risk control classification, proactive controls and reference.

a. CRC.T1: Risk Control Classification

D2 CRF, D3 TRMF, D5 ISP and D6 CSP discussed on risk control classification. The following Table 4.5 showed the similarities and differences of risk controls classification for the four documents.

Table 4.5 Risk Control Classification

Risk Control Classification		Document Name			
		D2 CRF	D3 TRMF	D5 ISP	D6 CSP
People	Cyber risk culture (awareness, education to BOD, management, staff)	/	/	/	x
	Human Resources	/	/	/	x
Process	Governance	/	/	/	/
	Asset management	/	/	/	/
	Third party management	/	/	/	/
	Physical & Environmental	/	x	/	x
	Incident management	/	/	/	x
	Information lifecycle management	/	/	/	/
	System security	/	/	/	/
	Network security	/	/	/	/
	Endpoint security	/	/	/	/
	Patch & Vulnerability management	/	/	/	/
	SSDLC	/	/	/	x
	Risk Management	/	/	/	/
	Due Diligence	/	/	x	/
	Backup & Recovery	/	/	/	/
	Change management	/	/	/	/
	Exit strategy	x	x	x	/
	Data classification	/	x	x	/
	Periodic inspection/audit/compliance	/	/	/	/
	Communications and operations management	x	x	/	x
	Information system acquisition, development and maintenance	x	x	/	x
	Business continuity management	x	x	/	x
	Cybersecurity strategic plan	x	x	x	x
Technology	VAPT	/	/	x	x
	Threat Intelligence	/	/	/	x
	Access control	/	/	/	/
	Cryptography	/	/	/	/
	Data loss protection	/	/	/	x
	SIEM	/	/	/	x
	Web Application firewall (WAF)	/	/	/	/
	Mobile device protection	/	/	/	x
	Cloud protection	/	x	x	/
	SOC	x	x	x	x
	Tool enhancement	x	x	x	x
	EDR	x	x	/	x
	NDR	x	x	/	x
Others	Resource & capacity planning	x	/	x	/
	IT strategy	x	/	x	x
	IT project management	x	/	x	x
	Financial management	x	/	/	x

From Table 4.5, risk control classification is comprised of people, process, technology, and others. People, process, and technology and their subclassifications aid

to the creation of Classification component in the framework. Others classification is not related to cyber security but related to technology control. Others classification is not part of the framework as it is not related to cyber security.

b. CRC.T2: Proactive Controls

D1 CSP, D2 CRF, D3 TRMF, D4 CRMF, D5 ISP, D6 CSP, D7, D8, D9 and D10 have identified the relevant proactive controls that contributes to the Proactive Controls component of the framework. One of the proactive controls is cybersecurity awareness and training. However, awareness and training are only focusing on staff, board members and management. It is not specified on awareness or training for customer and third party (i.e. vendor, agent). The absence of the awareness and training to customer and third party may cause incidents like D7.2, D8.1 and D10.

c. CRC.T3: Risk Control Reference

Refer to analysis in CRI.T4. The risk control reference is similar to risk identification reference.

d. CRC.T4: Challenges & recommendations

There is no specific document that specify the challenges in implementing cyber risk controls and recommendations to address the challenges.

4.3.3 General (G)

Documents being analysed discussed on landscape and trend of cyber threats and attacks. It also relates to cyber threats in emerging technologies and cybersecurity strategic plan operation.

a. G.T1: Cyber threats landscape and trends

Cyber threats landscape and trend of attacks are discussed in D7.1, D8.1, D9 and D10, which are related to DDoS attacks, third-party threats, phishing attacks and fraud.

Both incidents from D7.2 and D8.1 are caused by third party (bank agent and vendor). Continuous cyber security awareness programs for third parties should be conducted to be consistent with awareness programs conducted on staff. A further study on the cyber security awareness program's effectiveness could be explored.

There is a decreasing trend of staff clicking phishing links and submitting personal information based on phishing campaigns from 2021 until 2022. Continuous cyber security awareness programs for staff may help reduce the trend. However, a further study on the effectiveness of the cyber security awareness program could be explored.

The increase in fraud cases among banking customers through internet banking and mobile banking is common among banks. It is not an isolated case for certain banks only. Fraudsters are targeting customers to exploit human psychological weakness to obtain illegal financial gain. Continuous cyber security awareness programs for customers should be conducted to be consistent with awareness programs conducted for staff. A further study on the cyber security awareness program's effectiveness could be explored.

D4 CRMF and D6 CSP discussed cyber threats on the cloud. It also discusses risk identification and controls for cloud technology. D6 CSP is a policy that translates the risk and controls in the D4 CRMF framework into a workable process. It is in line with Aldasoro et al., (2022) view that the broader use of cloud services exposes the financial sector to cyber-attack cases. No documents about emerging technologies such as blockchain or IoT are specifically discussed. It is likely because of the bank's broad adoption of cloud technology for non-critical systems such as email, collaboration tools and corporate web portals. This is aligned with expert interview analysis, which mentioned that the bank established a cloud adoption strategy to ensure secure cloud implementation.

DDoS attacks, third-party threats, phishing attacks, fraud, and cloud, contribute to the risk identification component of the framework.