SECURITY RISK MANAGEMENT FRAMEWORK FOR ISO/IEC 27050 STANDARD

A THESIS SUBMITTED TO AUCKLAND UNIVERSITY OF TECHNOLOGY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

Supervisors

Prof Brian Cusack

Dr Alan T. Litchfield

November 2023

By

Nabeel Ali Mahfood Albahbooh

School of Engineering, Computer, and Mathematical Sciences

Declaration

I hereby declare that this submission is my work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning, except where explicitly defined in the acknowledgements.

Nabeel Ali Mahfood Albahbooh

Acknowledgements

It has been an amazing experience working on this study for almost four years (i.e., 2019 - 2023). I have completed my Doctor of Philosophy (PhD) study at the Faculty of Design and Creative Technologies of the Auckland University of Technology (AUT). I am very glad that this journey has come to an end. During my research, I have gained more knowledge, learned new skills, developed new ideas, and had fresh perspectives. I would like to thank numerous people for devoting their time, offering valuable guidance, and providing unwavering encouragement throughout the entire of my PhD study.

Words cannot express my gratitude to my supervisor Prof Brian Cusack for his invaluable advice, continuous support, and patience during the completion of the research. This extensive knowledge and plentiful experience have encouraged me all the time to finish the requirement. Additionally, I would like to thank Dr Alan Litchfield for his continuous support during my research proposal presentation and review of my thesis with valuable feedback that improved the research quality.

Thanks to AUT staff who helped and supported me during the COVID-19 pandemic. Special thanks to the AUT librarians, research assistants, and study participants who deserve special recognition and appreciation.

I am also grateful to my friend Dr Eghbal Ghazi Zadeh for his unconditional support, feedback sessions, and useful advice.

Lastly, my family deserves endless gratitude: my father for teaching me how to support people, my mother for teaching me how to be a role model, my lovely wife for taking care of our children while I am writing this thesis, and my innovative children for sacrificing their fun time to focus on my study.

Abstract

The purpose of the research is to add value for users to the recently released international standards and guidelines for Electronic Discovery (eDiscovery) by providing a security risk evaluation framework for users. At present, the eDiscovery guidelines ignore security risks and are populated by technical assistance for eDiscovery. The use of these guidelines without a security risk evaluation framework puts the users and the information at risk of disclosure and damage. The intention is to design an effective security risk evaluation framework and then test it through scenarios and expert feedback.

The Design Science Research Methodology (DSRM) is selected and adapted to guide this study and to systematically shape and improve the framework artefact. The research is primarily theoretical research that seeks to design a risk mitigation solution for eDiscovery investigators. The DSRM is enhanced by adopting sub-methods to fill gaps in the overarching methodology for systematically modelling the risks and quantifying the risks in eDiscovery practices as described in the ISO/IEC 27050 standard. The research is designed to follow three iterations for the theoretical design of an artefact, the testing, and the quality improvement.

The benefit of the research is for legal businesses and government departments where the adoption of eDiscovery standards and guidelines is mandatory. The current ISO/IEC 27050 standard does not have any sort of security risk framework. This research aims to fill the gap by designing a novel framework and guidelines for use. The added value of the proposed framework model is a shift from a requirements standard control approach towards an action-oriented and referenced approach. The proposed framework will be used to evaluate the ability of organisations to meet the objectives of security risk management when using the ISO/IEC 27050 standard. The proposed security risk framework discussed in this research will enhance their capability to manage a secure eDiscovery process. Selecting a fit-for-purpose framework is a challenge for most organisations. This research suggests the use of Artefact 3 as a practical guideline. Organisations might choose an integrated framework by mapping specific controls between two or more frameworks (e.g., use a combination of ISO/IEC 27050 and other security standards) to meet their compliance requirements and business needs. However, eDiscovery has specific security requirements that are not adequately defined in more general standards and guidelines. ISO/IEC currently offers 46 related security standards. The amount of information may be excessive when it comes to ready and active policies

and procedures to assure safe eDiscovery practices. This research introduces Artefact 3 as a proposed solution to address this problem.

The research derives the following questions from the literature to guide the artefact development and to fill a research gap.

Research Question: ***What framework aligns the current ISO/IEC 27050 standard with the ISO security risk evaluation framework in a cost-effective way?***

- **SQ1**: What are the main limitations and weaknesses of the current ISO/IEC 27050 standard in the context of risk management processes?
- **SQ2**: What design components improve the risk identification capabilities of the current ISO/IEC 27050 standard?
- **SQ3**: What steps are necessary to integrate the new artefact with the current ISO/IEC 27050 standard?

Feedback for experts on the proposed framework indicates that approximately two-thirds finds its components clear and relevant, while the majority considering it as useful for their workplace. Approximately 80% believe it aligns with international security risk management standards and will enhance risk management. However, 20% express concerns regarding both clarity and usability. Additionally, less than half of the feedback suggests the need for improvements, while 75% recommend specific adjustments to the artefact components.

In general, the proposed framework model's added value was evaluated through industry-specific usability testing. Expert feedback on Artefact 2 provided valuable insights into its perceived value during practical application. Subsequently, this feedback was meticulously analysed, leading to the incorporation of necessary modifications into Artefact 2 to better align with these insights. Artefact 3 now awaits piloting real-world testing in various contexts, with a focus on assessing its broader practical utility.

The thesis is structured in a standard format with seven chapters, a references list, and appendices.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ADSRM	Adaptive Design Science Research Method
ALE	Annualised Loss Exposure
BPM	Business Process Model
CF	Contact Frequency
CIRA	Conflicting Incentives Risk Analysis
COBIT	Control Objectives for Information and Related Technologies
CORA	Cost Of Risk Analysis
CORAS	Construct a platform for Risk Analysis of Security Critical Systems
DFD	Data Flow Diagram
Diff	Difficulty
DoDAF	Department of Defense Architecture Framework
DS	Design Science
DSR	Design Science Research
DSRM	Design Science Research Methodology
DSRP	Design Science Research Process
eDiscovery	Electronic Discovery
EMR	Electronic Medical Record
ENISA	The European Union Agency for Cybersecurity
ERMF	ENISA Risk Management Framework
ESI	Electronically Stored Information
FAIR	Factor Analysis of Information Risk
IAF	Integrated Architecture Framework
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISF	Information Security Framework
ISO	International Standards Organisation
ISRA	Information Security Risk Assessment
ISRAB-BM	Security Risk Analysis Based on a Business Model
ISRAM	Information System Security Risk Management
ISRAM	Information Security Risk Analysis Method
IT	Information Technology

ITIL	Information Technology Infrastructure Library
LEC	Loss Exceedance Chart (LEC)
LEF	Loss Event Frequency
LM	Loss Magnitude
NIST	National Institute of Standards and Technology
NSMROS	The Norwegian National Security Authority Risk and Vulnerability Assessment
NWIP	New Work Item Proposal
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PDCA	Plan-Do-Check-Act
PhD	Doctor of Philosophy
PL	Primary Loss
PoA	Probability of Action
RMF	Risk Management Framework
ROI	Return on Investment
SL	Secondary Loss
SLEF	Secondary Loss Event Frequency
SLM	Secondary Loss Magnitude
TAR	Technology Assisted Review
TC	Threat Capability
TEF	Threat Event Frequency
TOGAF	The Open Group Architecture Framework
Val IT	Value Information Technology
Vul	Vulnerability
WTO	World Trade Organisation

Chapter 1: Introduction

1.0 INTRODUCTION

Best practices have evolved from business responses to the legal standards for Electronic Discovery (eDiscovery). Many organisations are actively seeking a secure approach to performing the eDiscovery process for different use cases and impending litigation. In the case of a commercial investigation, it is expected that legal teams incorporate the discovery compliance obligations and the applicable laws or state rules. Courts expect organisations to apply judiciously and systematically a set of rules and principles within an eDiscovery process that is repeatable and defensible.

The physical location and types of Electronically Stored Information (ESI) continue to evolve, and organisations must embed an eDiscovery process across not only information stored on their premises (e.g., repositories, email, and servers), but also personally owned devices, social media platforms, and data stored in the cloud. This introduces a new challenge to various stakeholders including data owners, technical teams, legal investigators, and business owners. A well-defined security risk management framework should be in place to ensure that relevant ESI during the legal investigation process is preserved, reviewed, and produced in a compliant and secure manner. A framework enforces a set of practices during the litigation hold, identification, preservation, and collection processes, as well as during the review and production phases of investigation. For example, organisations should establish a defensible process by regularly verifying that the legal hold is being correctly enforced. This legal hold prevents any attempts to destroy evidence, penalties, and unforeseen events in the courtroom.

Therefore, this study focuses on finding solutions to ensure the eDiscovery process is followed securely. The overall objective of this research is to provide a well-defined security risk management framework that can be integrated into eDiscovery professional practices. It is achieved through a systematic approach by interlinking the appropriate attributes and relevant features of security risk management into the eDiscovery processes.

This chapter is split into six main sections. Section 1.1 provides background to the study, the gap, and why organisations need to have a risk management framework for eDiscovery. The current research issue and the purpose of this study are addressed in Section 1.2. Both Section 1.1 and Section 1.2 are further elaborated in Chapter 2 and Chapter 3. Section 1.3 defines the primary research question and three sub-questions. It

also presents three hypotheses to support the sub-questions. Section 1.4 presents the chosen research methodology from both theory and practice points of view. Chapter 3 has dedicated sections to explain more about the research question and the selected research methodology. The research contributions to the body of knowledge are discussed in Section 1.5 and further detailed in Chapter 6. Lastly, the overall thesis structure and research workflow are briefly reviewed in Section 1.6.

1.1 CONTEXT OF STUDY

eDiscovery is the electronic aspect of identifying, collecting, and producing ESI evidence in response to a request for evidence in a lawsuit or investigation. eDiscovery offers a best practices framework for investigations, evidence acquisition, and handling activities. The ISO/IEC 27050 standard describes the essential rules and steps for identifying and preserving relevant ESI when an investigation is initiated. It aims to ensure compliance with jurisdictions, courts, and regulation requirements, including civil and criminal proceedings, investigations, and audit purposes.

The ISO/IEC 27050 series provide a set of guidelines on how to handle ESI and support eDiscovery through seven main processes: identification, preservation, collection, processing, review, analysis, and production (Arshad et al., 2020; Nieto et al., 2017). The ISO/IEC 27050 standard also provides a legal perspective as part of the eDiscovery lifecycle. It does not conflict with or override the laws and regulations of a specific jurisdiction. Instead, it assists ESI investigations, evidence acquisition, and handling processes (Bhatia & Malhotra, 2020).

Risk management aims to establish preventive and control measures that effectively address the risks associated with particular activities and valuable assets. By promptly identifying potential risks, organisations can develop plans to minimise the potential impact (Barateiro et al., 2012). The risk management process encompasses a structured set of activities for proactively identifying and mitigating risks. By employing this process, organisations effectively manage the risks by establishing the context for risk, identifying, evaluating, reviewing, treating (applying measures), and monitoring risk to minimise threats and vulnerabilities. This approach also enables organisations to quantify risk for acceptance. The existing risk management frameworks are designed for specific industry requirements such as telecommunications service providers (Mayer & Aubert, 2020) and SCADA systems (Cherdantseva et al., 2016). Hence, the task to set criteria or common properties for selecting a fit-for-purpose risk management

methodology from a range of choices is possible for specific contexts. Since this research focuses on literature that is relevant to information security, five leading risk management frameworks have been chosen in this context: ISO/IEC 31000:2018 Standard, ISO/IEC 27005:2022 Standard, NIST Risk Management, The European Union Agency for Cybersecurity (ENISA) Risk Management, and The Risk IT Framework.

This research holds benefits for businesses and government departments where the adoption of eDiscovery standards and guidelines will be mandatory. The proposed security risk framework aims to enhance their capability to manage a secure eDiscovery process. Selecting a fit-for-purpose framework is a challenge for most organisations. Organisations might select an integrated framework by mapping specific controls between two or more frameworks (e.g., use a combination of ISO/IEC 27050 and other security standards) to meet their compliance requirements and business needs. Therefore, this study adds value to the recently released standards and guidelines for eDiscovery by providing a security risk evaluation framework for users. At present, the eDiscovery guidelines ignore security risks and are populated by technical assistance for discovery. The use of these guidelines without a security risk evaluation framework puts the users and the information at risk of disclosure and damage. The objective of this study is to design an effective security risk evaluation framework and subsequently test its efficiency.

1.2 THE PROBLEM

The problem addressed in this research comes from the literature review process which has identified a gap that exists within the ISO/IEC 27050 standard. It shows that the ISO/IEC 27050 standard establishes the specifications and guidelines for the process of discovering ESI or data by one or multiple parties involved in an investigation, legal dispute, or similar legal proceedings. It has no security provisions for information protection. Moreover, the current ISO/IEC 27050 standard does not have any sort of security risk framework.

This research investigates defining a security risk management framework applied to the ISO/IEC 27050 standard to provide mechanisms that allow organsiations to evaluate their ESI security risk. Although the ISO/IEC 27050 standard helps in identifying the risks associated with eDiscovery and then providing a basic mitigation plan, it does not provide a detailed description of how to identify risks and manage them. Instead, it provides high-level requirements for the whole ESI investigation process.

These limitations motivate the researcher to review the current literature in the body of knowledge on security risk management.

This research develops a risk management reference model to assess the current state of the ISO/IEC 27050 standard in terms of its capabilities to manage security risk. Hence, the research aims to fill the gap by designing a novel framework and guidelines for use. The added value of the proposed framework model is a shift from a requirements standard control approach towards an action-oriented and referenced approach. The proposed framework evaluates the ability of an organisation to meet the objectives of security risk management when using the ISO/IEC 27050 standard. It protects from libellous attacks and achieves protection despite potential attack and security incidents. Furthermore, the proposed framework defines a set of processes that manage and measure for control of all aspects of security risk. It relies on indicators for benchmarking and supports understanding of the security risk requirements of an organisation. These indicators are specifically designed to align with the security needs of the organisation, ensuring that they are effectively met. It gives innovation and a security framework that will transform eDiscovery practices into a more trusted and secure process.

1.3 THE RESEARCH QUESTIONS

This research forms a primary research question based on the literature to solve the identified research problems and to achieve the research objectives. Moreover, the researcher formulates research hypotheses as statements of expectation that are evaluated and tested.

This research aims to respond to the gap and to address the opportunity by answering the primary question of this research: "**What framework aligns the current ISO/IEC 27050 standard with the ISO security risk evaluation framework in a cost-effective way?**". The sub-questions to clarify the primary research question are:

- **SQ1**: What are the main limitations and weaknesses of the current ISO/IEC 27050 standard in the context of risk management processes?
- **SQ2**: What design components improve the risk identification capabilities of the current ISO/IEC 27050 standard?
- **SQ3**: What steps are necessary to integrate the new artefact with the current ISO/IEC 27050 standard?

Answering the three sub-questions contribute to answering the primary research question. Furthermore, this research creates three hypotheses to support answering the previous sub-questions. The three research hypotheses are:

- **H_1**: The proposed framework model adds value with a shift from requirements approach to a referenced standards approach.
- **H_2**: The new artefact better identifies the risks associated with electronic discovery.
- **H_3**: The new artefact is a cost-effective risk identification method for organisations.

To test and measure the added value of the proposed framework model, the researcher strives to attain industry usability. Valuable insights into its practical worth are obtained from expert feedback on Artefact 2. The researcher analyses this feedback and incorporates the necessary adjustments into Artefact 2 to align it accordingly. Subsequently, Artefact 3 may require piloting in real-world scenarios to assess its value in wider contexts.

1.4 THE METHODOLOGY

The research focuses on the common area between eDiscovery and security risk management. The researcher needs to examine the relevant studies in these areas to comprehend the current literature as well as existing frameworks and industry standards. To accomplish that, the researcher chooses a research methodology from two perspectives: theory and practice.

From a theory perspective, Design Science (DS) is chosen to guide the research as the researcher needs to take a theoretical construct from the literature review and improve it. Each DS artefact produced as output is subjected to an improvement process based on internal testing and expert feedback input.

Design Science Research (DSR) consists of three main characteristics. It has conceptual principles to establish the definition and goals of DSR; practical guidelines to follow; and a structured process for conducting and presenting the research (Peffers et al., 2007). However, Design Science Research Methodology (DSRM) provides a formal process model for conducting DS and creating relevant artefacts.

This research uses a DSRM as a framework for guided action to deliver an artefact of value. The value is for both theory and practice. Therefore, based on DS and DSRM, the researcher selects an Adaptive Design Science Research Method (ADSRM) to define

the problem statement, design risk management framework artefacts; and ultimately produce a new solution. The ADSRM approach consists of six main phases as depicted in Figure 1.1. The method steps with the associated inputs, processes, and outputs are explained in more detail in Chapter 3.

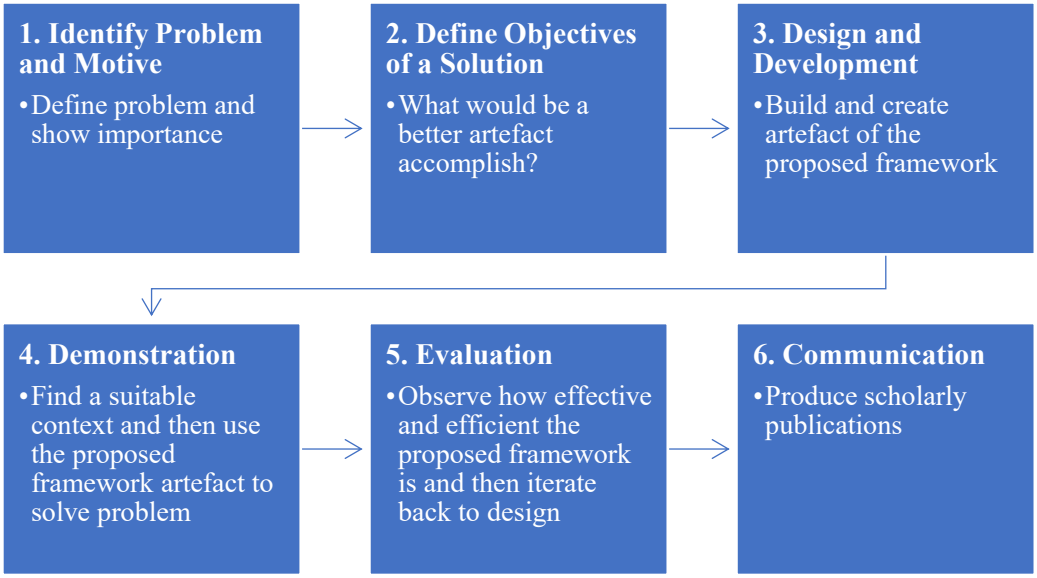


Figure 1.1: Adaptive Design Science Research Method

Moreover, the primary objective of the ADSRM approach is not only to create an artefact but also to address research questions. This research shapes a set of processes to deliver novel outcomes.

On the other hand, from a practical perceptive, the overall research approach consists of five main steps as depicted in Figure 1.2.

Figure 1.2: Research Approach

At the start of this research, the researcher performs document analysis that focuses on reviewing and evaluating the current ISO/IEC 27050 standard series (Part 1, 2, 3, and 4). The data within this standard undergoes analysis and interpretation to produce significance, acquire comprehension, and develop new knowledge. Moreover, document analysis involves a content analysis process in which data are categorised into groups based on the key questions of this research.

In the second step, the researcher conducts a comprehensive study to have a better understanding of various aspects relevant to the research interest. The study includes the following aspects:

- Perform a general study to gain a better understanding of the current ISO/IEC 27050 standard.
- Describe the required knowledge, structure, and artefacts of ISO/IEC 27050 standard.
- Study and identify the limitations and weaknesses of the current ISO/IEC 27050 standard in the context of information security.

In the third step, the researcher carries out an intensive study to build and propose an effective security risk management model to fulfil the current gaps within the ISO/IEC 27050 standard as follows:

- Identify the gap with the current ISO/IEC 27050 standard in the context of security risk management.
- Identify the main components and artefacts of the proposed framework model.
- Design and develop the proposed framework model based on international best practices.
- Integrate the proposed framework model into the ISO/IEC 27050 standard.

In the fourth step, the researcher assesses and evaluates the effectiveness of the proposed framework model, and then recommends appropriate enhancements as follows:

- Conduct various scenarios testing of real stories.
- Develop a template for feedback questions.
- Share the proposed framework model with a group of experts for their opinion and feedback.
- Analyse and evaluate the effectiveness of the proposed framework model.
- Suggest future improvement and work.

In the final research step, the researcher communicates the research outcomes to researchers and relevant audiences in the form of a Doctor of Philosophy (PhD) thesis publication as well as Journal articles and Conference papers.

1.5 THE CONTRIBUTION

The thesis contributes to the body of knowledge in both theory and practice. In theory, the researcher creates an adaptive research process based on the combinations of both

DSRM and DSRP methodologies with adjustments. The proposed framework was utilised to address risks in the eDiscovery process by applying it to three scenarios extracted from existing literature. A DS investigation is an exploratory methodology where an artefact is produced, reviewed, evaluated, and improved. This research answers the defined research questions with three supporting sub-questions. The researcher tests the proposed framework using a qualitative approach. The last step of this research demonstrates the primary results in the form of a PhD thesis that covers the problem statement, review of relevant literature, formulation of hypothesis, data collection and analysis, presentation of results, comprehensive discussion, and concluding remarks. In the future, the data and framework can be published in the form of a Journal articles and Conference papers.

On the other hand, in practice, eDiscovery investigators in government agencies and legal offices can use the proposed framework to conduct investigations, acquire evidence, and handle ESI more safely and consistently than by relying solely on traditional methods, such as chain of custody. eDiscovery investigators follow rules and steps to identify and preserve relevant ESI when an investigation is initiated to meet various investigation requirements. The security risk is controlled and managed using the proposed framework that is tailored to the eDiscovery processes. The testing scenarios simulate real-life situations and reinforce the concepts and approaches presented in the research. The three scenarios are:

1. The process of searching, locating, and securing ESI to use it as evidence in a legal case.
2. The issue of data leakage arises for organisations when they store the intellectual property (IP) of third parties across multiple locations.
3. The risk implications of inconsistent medical records arise when data are transferred between actors and organisational units.

Moreover, a selected group of experts evaluates the proposed framework. The data collected through expert feedback confirms that the proposed artefact is valuable for identifying and managing risks in the eDiscovery domain.

1.6 THESIS STRUCTURE

The thesis is structured into seven chapters as follows. Chapter 1 provides an overview of the research with a background to the study and why it is important. This chapter also highlights various aspects including the purpose of the study, the current research issue,

the research questions, the research methodology, the contribution to the knowledge and practice, and the structure of the remainder of the thesis.

Chapter 2 provides a comprehensive literature evaluation of the existing risk management frameworks. A summary of five selected risk management frameworks is presented. These are ISO/IEC 31000, ISO/IEC 27005, NIST, ENISA, and The Risk IT. Furthermore, this chapter explores basic probabilistic concepts that are essential for reviewing the existing risk management frameworks. More specifically, it identifies the current issues with the ISO/IEC 27050 standard and highlights the gaps. Subsequently, it presents a set of concerns that must be addressed to fill in the identified gaps.

Chapter 3 starts by presenting the concept of DS and describing two well-known methodologies. The fundamental concept behind DSR is that knowledge and comprehension of a design problem and its resolution are obtained during the development of an artefact. It justifies the choice of the methodology. An adaptive version of two DSR methodologies has been created to meet the research requirements. Furthermore, this chapter follows a problem-solving approach that includes formulating a hypothesis or proposition, designing an adaptive research methodology, describing a theoretical framework (Artefact 1), collecting data, validating the hypothesis, analysing the obtained results, and then drawing conclusions that can later be assessed by independent domain experts. Additionally, this chapter explains the supporting tools used to model and conduct the risk analysis including Monte Carlo simulation, FAIR-U risk calculator, and Archi model designer. The last section of this chapter discusses the limitations of this research.

Chapter 4 describes three testing scenarios to help the researcher understand the framework in action and context. These scenarios focus on evaluating the security risk of eDiscovery when collecting electronic content for legal cases, protecting third-parties IP from data leakage, and minimising Data inconsistency with medical records. This chapter uses the outcomes of the scenarios tests to improve the proposed framework and create Artefact 2. Furthermore, it presents an architecture modelling of Artefact 2 with a set of graphical notation, and relationships based on ArchiMate 3.1 metamodel.

Chapter 5 evaluates Artefact 2 through expert feedback. It discusses the results of two types of evaluation: naturalistic expert evaluation and Artefact thematic evaluation. Then, it presents the improved version of the proposed framework (Artefact 3), focusing on its integration with eDiscovery processes, key principles, framework style, process, and ArchiMate 3.1 metamodels.

Chapter 6 discusses the research findings to provide answers to the three research sub-questions based on the literature review, artefact development, testing, and evaluation. This is followed by a discussion of each of the hypotheses tested and the results of the tests. Then, this chapter uses both sub-question answers and hypothesis testing to answer the primary research question. Furthermore, this chapter discusses how the research results are related to the existing literature and explores their implications to identify the research contribution in both theory and practice.

Chapter 7 concludes the research and begins by summarising the research. It also presents the contributions to knowledge, explains the limitations of the study, and then concludes with recommendations for future research.

At the end of this thesis, a detailed, alphabetical list of all the sources cited in the thesis is provided, and the Appendices contain supporting documents, including the ethics approval to do the research, an introduction letter for expert participation, the template for expert opinion, and expert feedback records.

Figure 1.3 maps the methodology to the three Artefacts by page number.

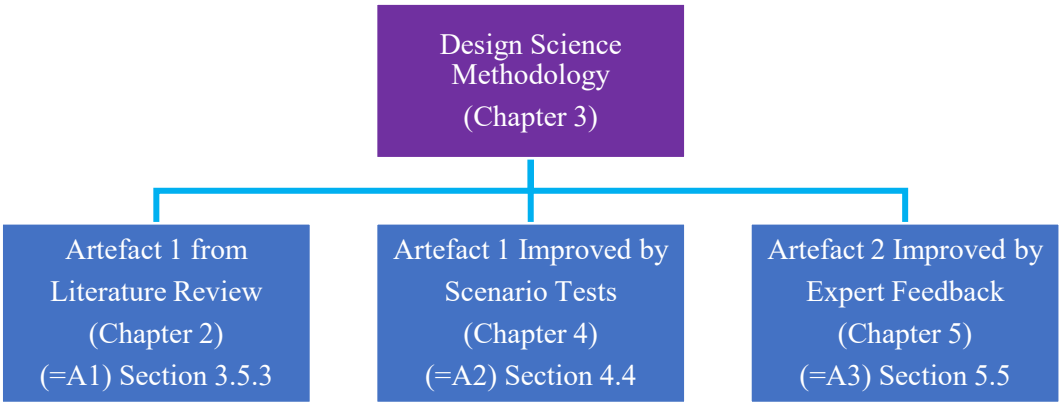


Figure 1.3: Methodology High-Level and Artefacts Mapping

In each chapter, Figure 1.4 is represented again with dashed lines for the chapter content and progress. This allows the reader to effectively track the execution of the methodology and understand each process involved in designing, testing, and evaluating the Artefacts. Each phase consists of a step or a set of steps, and the arrows indicate a transition from one phase to another as follows: Problem Identification and Definition (Chapter 2), Solution Objectives Definition (Chapter 2), Artefact Design and Development (Chapter 3), Artefact Application Demonstration (Chapter 4), Demonstration Effectiveness Evaluation (Chapter 5), and Artefact Results Communication (Chapter 6 and Chapter 7).

The mapping between the ADSRM approach of the thesis chapters is illustrated in Figure 1.4. It maps the research methodology phases with each chapter of the thesis.

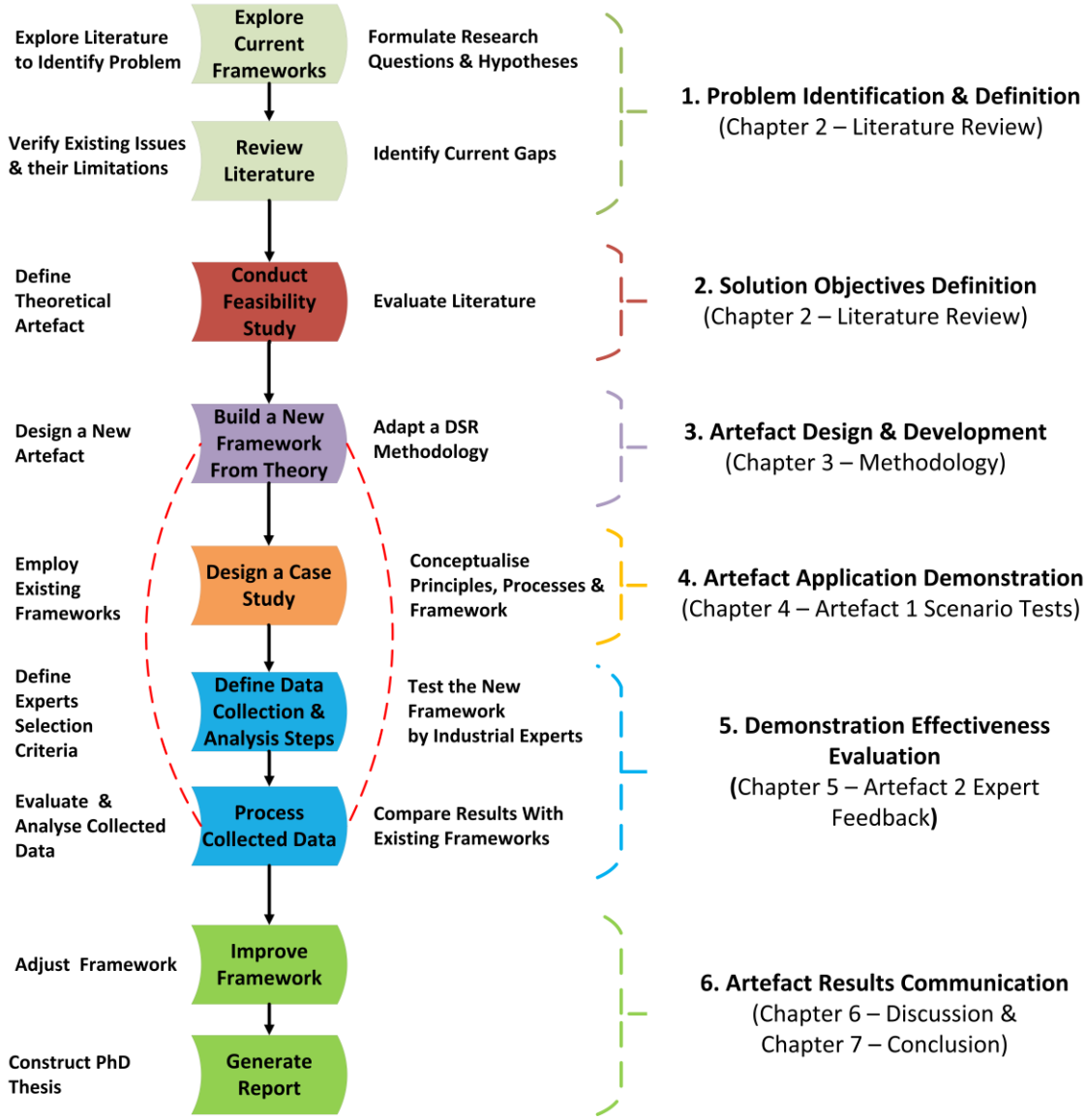


Figure 1.4: Research Methodology and Thesis Chapters Mapping

Chapter 2: Literature Review

2.0 INTRODUCTION

Figure 2.1 illustrates the summary of the thesis structure based on the proposed research methodology. The dashed lines show the roadmap for Chapter 2 which is Phase 1 (Problem Identification and Definition) and Phase 2 (Solution Objectives Definition).

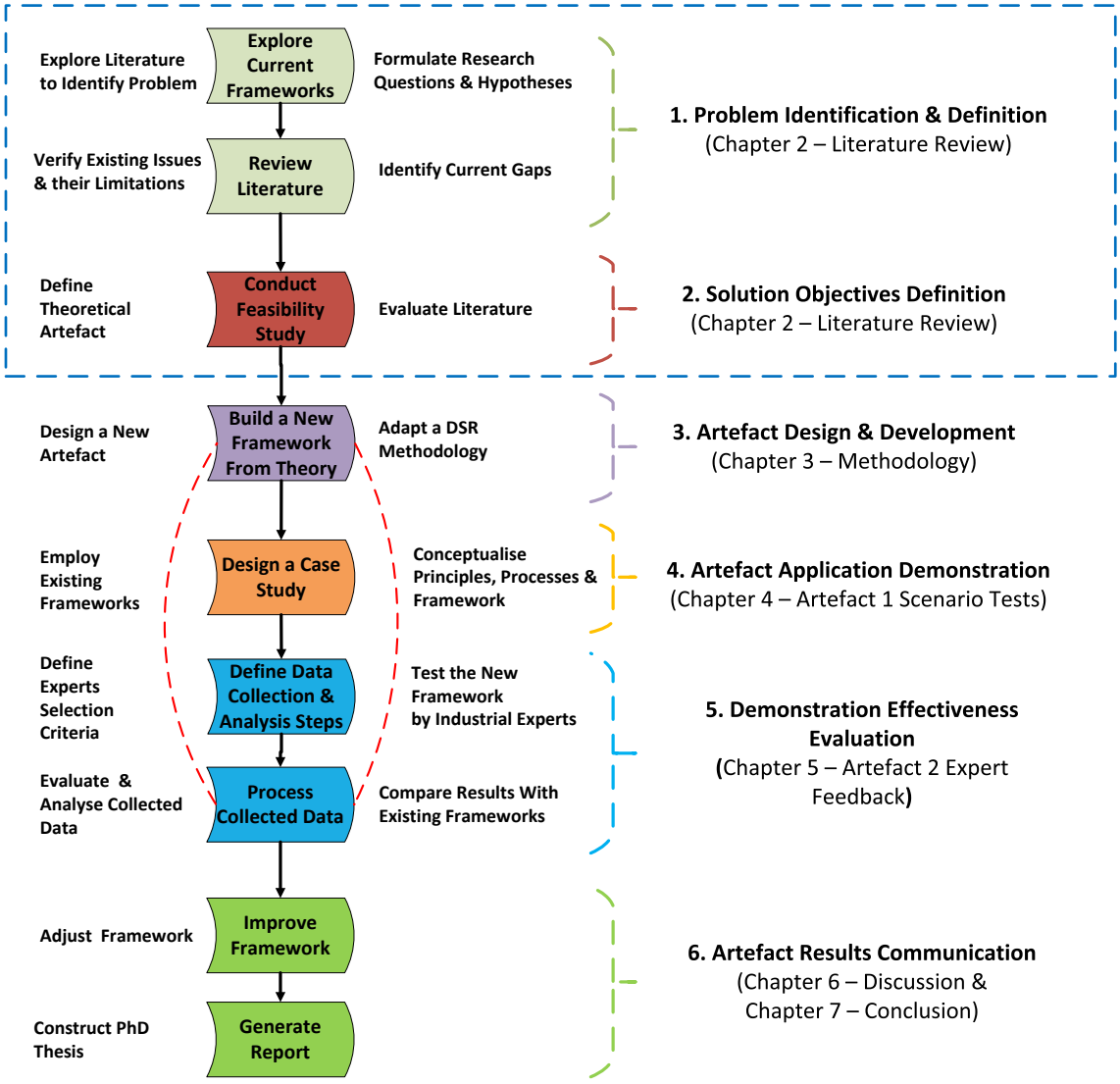


Figure 2.1: Chapter 2 Roadmap

The literature review plays a major role and a foundation for this research. It serves as the grounds for the research theory identities and the research gaps (Snyder, 2019).

In this research, a literature review is employed as a method for synthesising research findings to provide the basis for building a new framework or conceptual model as described in Chapter 3. The review aims to summarise previous research, maps and

assesses the findings, and justifies the primary research question, sub-questions, and hypotheses. Furthermore, the literature review evaluates the state of knowledge on risk management frameworks by searching and filtering information, creating research agendas, and then identifying gaps (Snyder, 2019; Torres-Carrión et al., 2018). A comprehensive review of the risk management frameworks is made and a summary of five selected risk management frameworks is presented.

Chapter 2 is organised as follows. Section 2.1 defines the ISO standard terminology and then identifies its value and challenges for organisations. It also describes the development lifecycle of the ISO formal standard. Section 2.3 describes the process used to conduct the literature review using the researcher's selection method. By employing this method, the researcher can effectively identify and decompose the data to identify any gaps or issues within the scope of the research. The selection process involves pre-evaluating research papers from the higher-ranked Journals to determine the most relevant articles for inclusion.

Section 2.4 presents a definition of risk in the context of ISO standards followed by a high-level discussion about the evaluation criteria of risk management frameworks. In addition to that, five selected risk management standards are evaluated, followed by artefact baseline mapping of the selected frameworks. Section 2.5 provides details about the ISO/IEC 27050 standard series and its framework. Further details about the current research on standards and standardisation are presented in Section 2.6. Then, the current issues and problems are summarised in Section 2.7, and the proposed solution is outlined. The chapter ends with the main conclusion and connection to Chapter 3 in Section 2.8.

2.1 THE VALUE OF STANDARDISATION

People and organisations have a misconception about standards, as they perceive them as something mandatory or obligatory to use or follow. However, the main purpose of standards is to provide valuable benefits to those who are using them. They provide competitive advantages that should motivate people and organisations to use them such as legalisation, regulation, or technical reasons (von Faber, 2014). The most significant advantage of standardisation is to have a common ground between different contexts in a particular domain.

2.2 STANDARDS AND STANDARDISATION DEFINITION

A standard is defined as a document created by a recognised organisation body to provide rules, guidelines, or characteristics for activities; and then achieves the optimum degree of direction for community benefits (Hatto, 2010). Standards are based on the consolidated results of three key components: science, technology, and experience.

On the other hand, standardisation is an activity that involves a set of processes for formulating, issuing, and applying standards to ensure the managed prevention of barriers to trade and the facilitation of technological cooperation (Hatto, 2010).

von Faber (2014) states that a standard has three main characterises as follows:

- **Approval**: Pre-approved, and demonstrably better than other solutions in general and therefore strongly recommended for application and adherence.
- **Recognition**: Widely recognised or employed, especially for consistency of outcomes.
- **Preference**: Preferred and automatically implemented if there is no serious objection.

In summary, the terms Standard and Standardisation embody the rules, guidelines, processes, and practices by which the safety, consistency, and quality of a product, service or activity are supported (Ogunsola & Mariscotti, 2013).

2.2.1 The Benefits and Challenges of Standardisation

Although standardisation is a slow process, requires resources and investments, and is an expensive task to implement, it offers numerous benefits to research and development areas such as finance, human resources, quality of products, innovation, environmental protection, and social responsibility. Primarily, it enhances both the performance and quality of product development and service delivery; and reduces operational costs through well-defined guidance. It also enables better communication between humans and organisations through global commitment, recognition, and acceptance. Moreover, it minimises product and service complexity which makes them manageable in large-scale environments and provides faster provisioning. Lastly, it supports various regulations relevant to practice (Anttila & Kajava, 2010; von Faber, 2014).

On the other hand, the standard is a useful tool for promoting innovation and commercialisation. It bridges the gap between different bodies and entities and then

connects research to the industry by distributing new ideas and practices, validating new measurement approaches, and applying new processes (Hatto, 2010).

2.2.2 Standards Development Lifecycle

Hatto (2010) describes the development lifecycle of ISO formal standards based on the ISO/IEC Directives Part 1 (Procedures for the Technical Work) and Part 2 (Rules for the Structure and Drafting of International Standards).

Figure 2.2 presents the process involved in developing the various international standard artefacts. It depicts a nine-stage lifecycle, starting from the proposal stage and ending at the publication stage.

Figure 2.2: Standard Development Lifecycle

In the first stage, a member body sends a New Work Item Proposal (NWIP) for initial evaluation. During the second stage and after three months, a ballot of members of a relevant technical committee is approved if at least five primary members agree to participate and more than 50% of those voting support the proposal. Once the NWIP is approved, it is recorded and registered in a database.

Then, a working draft submitted by the proposer is further developed by experts as part of the third stage. At the next stage (Stage 4), three months of review and ballot are conducted by members of a Technical Committee (i.e., it may take 2 or 4 months to reach the agreement). The outcome of this review is a final draft.

Once the final draft is ready, the first committee draft is conducted in the fifth stage. The committee sends comments and then receives a resolution of comments identified during this stage. Next, during the sixth stage, the final committee draft is produced. Publicly Available Specification and Technical Reports are published when a majority of those voting approve the document. Technical Specification is published if at least two-thirds of those voting approve the document.

Drafting international standards is performed through the formal route/enquiry stage (Stage 7). At this stage, five months of review and ballot are conducted by all members of ISO. The draft is approved if votes of at least two-thirds of the primary members of the committee responsible for the document are in favour and no more than a quarter of total votes are against (i.e., abstentions and negative votes not accompanied by technical reasons are not counted). Similarly, as in Stage 4, the committee sends comments and then receives the resolution of comments identified during this stage. Next, during the eighth stage, the final draft international standard is approved. Two months of review and ballot are carried out by all members of ISO. No comments are allowed except for negative votes for which technical reasons must be stated. The draft standard is approved if votes of at least two-thirds of primary members of the committee responsible for the document are in favour and no more than a quarter of total votes are against (i.e., abstentions and negative votes not accompanied by technical reasons are not counted).

Once the draft international standard is approved, the final stage of this process (Stage 9) is executed in which the draft document is officially published as an international standard.

The expected timeframe for approving the NWIP (Stage 2) to publishing the Technical Specification (Stage 6) is between 18 to 30 months, while the entire process (from Stage 2 to the final stage) from approving the NWIP (Stage 2) to publishing the international standard (Stage 9) is between 36 to 48 months.

2.3 LITERATURE SELECTION APPROACH

Snyder (2019) defines three literature review types: systematic review, semi-systematic review, and integrative review. These review types have specific criteria and can be applied to qualitative, quantitative, and mixed approaches, depending on the review phase. The systematic review helps researchers identify all relevant empirical evidence that meets the pre-specific inclusion criteria, thus addressing specific research questions or hypotheses. When reviewing academic literature (e.g., articles, journals, and papers),

bias can be reduced; thus, providing more independent justification in which conclusions can be drawn and a decision made (Snyder, 2019; Torres-Carrión et al., 2018). Since the systematic review is one of the most accurate methods to collect literature, the researcher has selected it to conduct the literature review for this study.

Snyder (2019) proposes a process for conducting a literature review that can be employed to develop a review that meets the criteria for research publications. This process consists of four main phases: design, conduct, analysis, and report as illustrated in Figure 2.3.

Figure 2.3: Literature Review Process Phases

This process has been selected and adapted to fit the research requirement as presented in Table 2.1.

Table 2.1: Literature Review Selection Criteria

Criteria	Description
Selection Method	Systematic approach
Review Method	Three rounds
Keywords	Risk management and framework-relevant keywords
Digital Library Search Databases	ACM, AIS, British Standards, Emerald Insight, Gartner, Google Scholar, IEEE, Science Direct, Elsevier, and Springer
Limitations	Articles published in English between 2000 and 2021 at a time of review
Groups of Interest	International risk management standards and comparative studies
Reporting Method	Systematic approach

Each of the phases depicted in Figure 2.3 is described in the subsections below.

2.3.1 Phase 1 – Literature Review Design

The main objective of this literature review is to explore and synthesise evidence regarding the impact of a specific factor. Therefore, a systematic review approach is employed to achieve this goal. This phase assists in identifying the primary research question and issues related to the research problem. The primary research question and

sub-questions (briefly discussed in Chapter 1 and detailed in Chapter 3) serve as a guide for gathering relevant academic literature.

During the design phase, a search strategy was used to identify all relevant academic literature. This includes selecting keywords and appropriate databases and deciding on including and excluding criteria as well as addressing limitations as previously explained in Table 2.1.

2.3.2 Phase 2 – Literature Review Conduct

In this phase, a technique called "Delphi" is employed to systematically structure and facilitate group communication. The Delphi technique has gained extensive usage in facilitating decision-making processes through the utilisation of experts' opinions. It systematically searches for the most reliable opinion from a group of potential options, typically comprised of experts or selected groups within the research scope. Furthermore, the Delphi technique is a questionnaire-based approach that facilitates the organisation and dissemination of opinions through iterative feedback. It has established a reputable presence in the field of Information Systems (IS) studies, serving as a valuable tool and a methodology for justifying the selection of literature. It is known to be a qualitative research technique with quantitative elements (Gallego & Bueno, 2014; Okoli & Nguyen, 2015). Using three rounds of the Delphi technique, in the context of this research, allows the researcher to focus on the research problem; and then systematically gather the latest and up-to-date scholarly publications.

The Delphi technique consists of four key elements: anonymity, iteration, controlled feedback, and statistical 'group response' (Gallego & Bueno, 2014). It has been found the Delphi technique is a useful tool to manage a large amount of general literature available in the topic scope and to select the relevant literature. The iterative rounds (i.e., up to three rounds) refined the target to a point the required themes were clear and the volumes manageable. Figure 2.4 depicts a researcher's literature review selection method for identifying gaps in previous research reports. This approach incorporates two key elements of the Delphi technique: iteration and controlled feedback.

Several approaches were involved in the selection of the articles, to manage the research scope. For example, researchers can read full-text articles that match the search criteria, but this method tends to be time-consuming. Alternatively, researchers can opt to focus on the research method, data analysis, and findings as a different approach. Moreover, researchers may choose to conduct the review in stages, initially focusing on reading abstracts and making preliminary selections. Subsequently, researchers read full-

text articles before finalising the selection. Next, the collected and relevant articles undergo a thorough screening to ensure they meet the inclusion criteria. In certain cases, references within the selected articles may also be scanned to identify other relevant articles in the research scope. It is important to highlight here that during the screening process, all included and excluded articles should be systematically documented (Snyder, 2019).

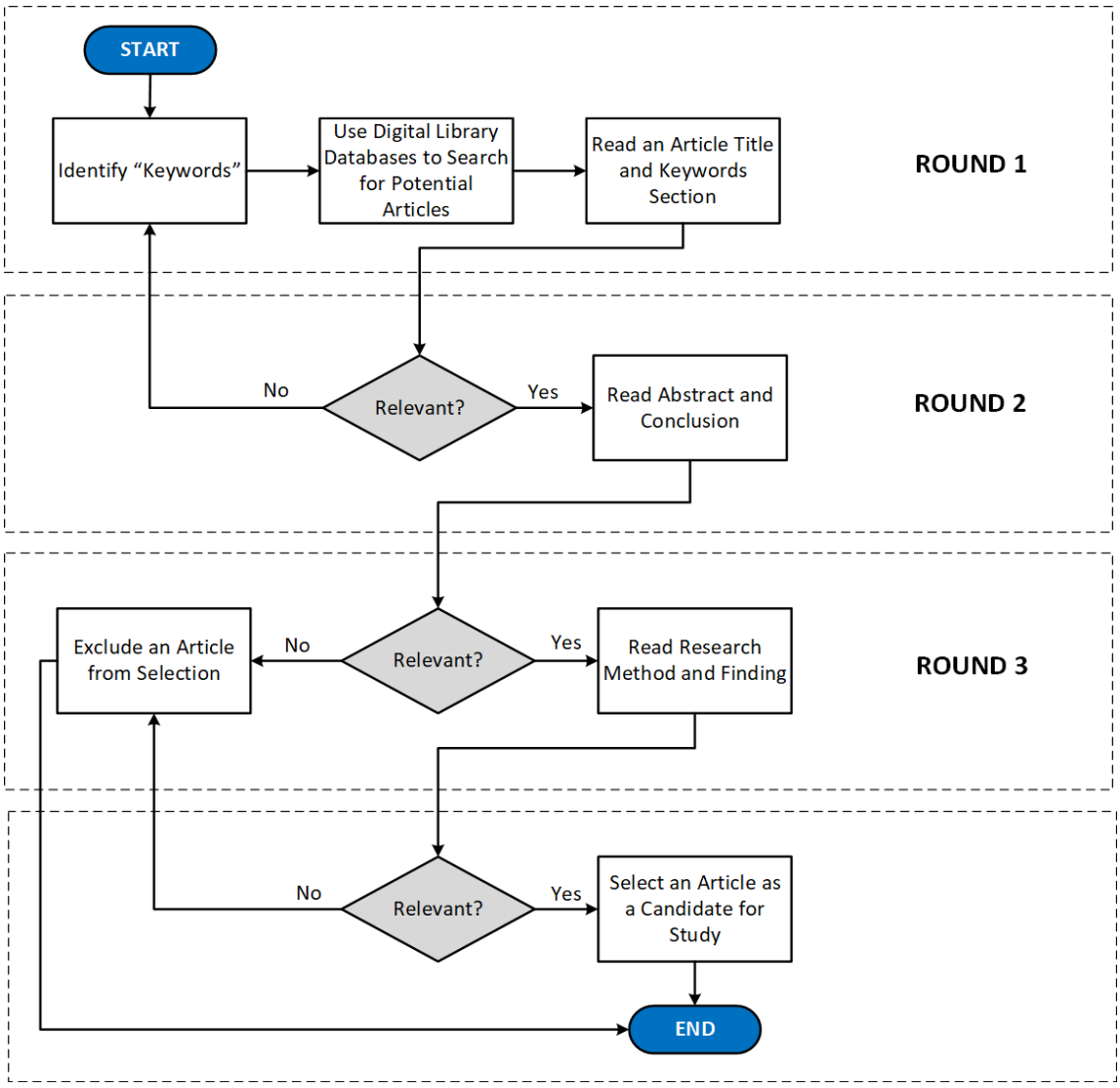


Figure 2.4: Researcher's Literature Review Selection Method

In the first round of this process, the "risk management", "risk management comparison", "risk management framework", "information security risk management", "enterprise risk management", "IT risk management", "risk assessment method", "risk model" and others are identified as keywords for the search scope. Those keywords are supplied in the "title" search section on the selected digital library search databases. A set of digital library search databases, including ACM, AIS, British Standards, Emerald

Insight, Gartner, Google Scholar, IEEE, Science Direct, Elsevier, and Springer is used to find the most relevant articles among thousands of academic articles. The selection is limited to the articles published between 2000 and 2021 which was he most recent at the time of research.

The second round focuses on checking the quality of the articles based on their abstract and conclusion, and relevance to the search questions. If the articles are relevant, then the third round is triggered by reading the research method and finding the articles. Finally, passing the previous three rounds allows choosing the articles as potential candidates for this research. If the articles are not relevant, then they are excluded from the selection during the second and third rounds respectively.

2.3.3 Phase 3 – Literature Review Analysis

After conducting the literature review in the previous phase and deciding on a final sample, a document analysis approach is used to perform further analysis. Figure 2.5 presents a literature review analysis method used to study and analyse the current risk management frameworks and then draft a conceptual model.

At the start of this research, a comprehensive study of the standards is conducted to get a better understanding of the various aspects relevant to the research objectives. These are:

- Perform a general study to gain a better understanding of the current ISO/IEC 27050 standard.
- Describe the required knowledge, structure, and artefacts of ISO/IEC 27050 standard.
- Study and identify the limitations and weaknesses of the current ISO/IEC 27050 standard in the context of information security.

Document analysis involves a content analysis process in which the selected articles are categorised into groups related to the primary research question. It also involves abstracting appropriate information from the selected articles.

During the classification step of this analysis, the selected articles are categorised into three key groups. Group 1 includes five chosen baseline risk management frameworks that are relevant to the information security discipline. For example, Control Objectives for Information and Related Technologies (COBIT) and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) frameworks have been excluded because either they are already aligned with other frameworks (e.g., COBIT aligns with the NIST and The Risk IT) or used in other frameworks (e.g., ENISA uses OCTAVE as

a baseline and adopts to its security controls catalogue). On the other hand, Group 2 covers articles that propose a customised framework based on international standards (e.g., Enterprise Risk Management was based on the ISO/IEC 31000 standard) or use common criteria to develop a new framework (e.g., ISRA was structured based on six risk management methodologies). Unlike Group 1 and Group 2, Group 3 contains four supportive frameworks related to the ISO/IEC 27050 standard which is the focus of this research. For example, ISO/IEC 27037, ISO/IEC 27040, and ISO/IEC 38500 standards interact with eDiscovery activities while the ISO/IEC 30121 focuses on risk management governance for digital forensics as illustrated in Figure 2.5.

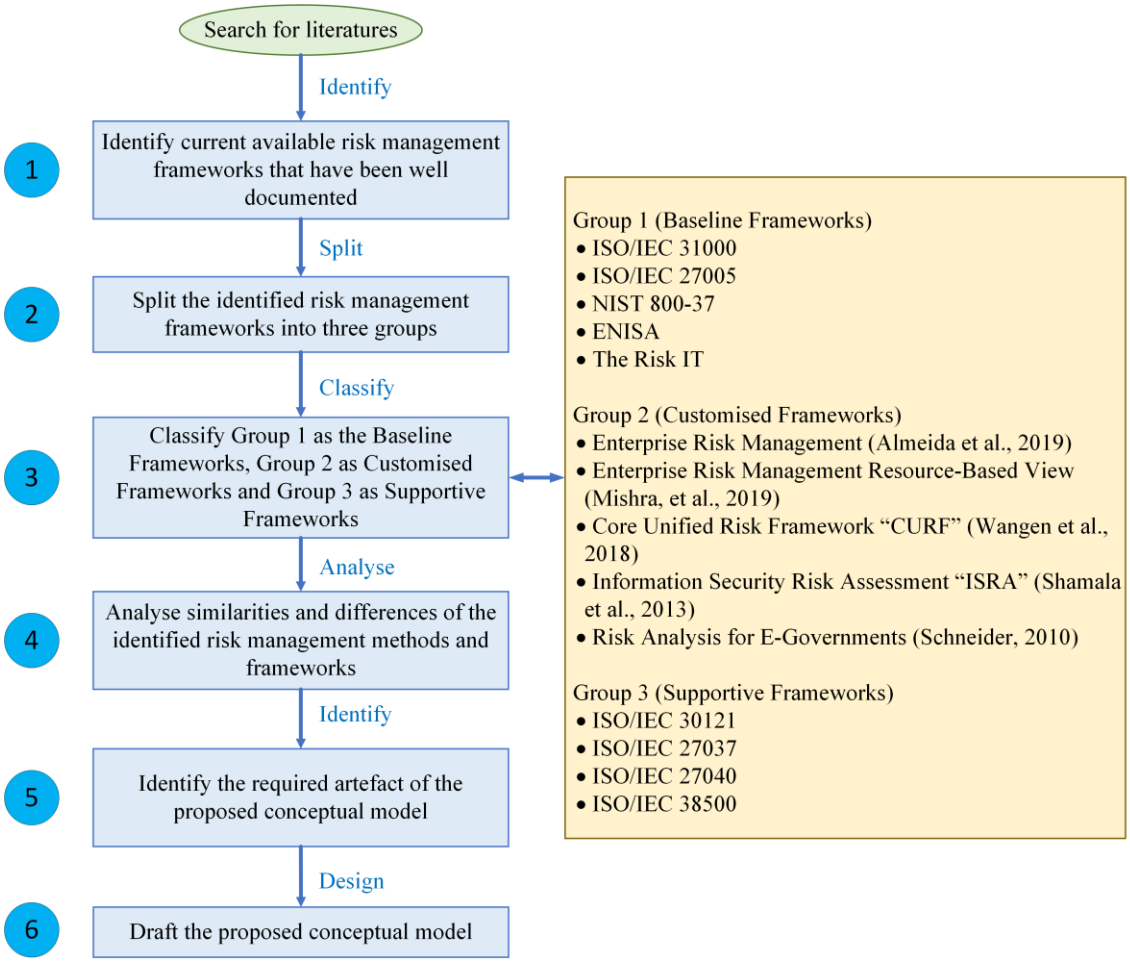


Figure 2.5: Literature Review Analysis Method

2.3.4 Phase 4 – Literature Review Report

There are many ways to structure and report the article status, depending on the collected information and the levels of detail. However, in this research, the reporting mechanism follows a systematic approach in which the following components are considered as listed and described in Table 2.2.

Table 2.2: Literature Review Report Components

Component	Description
Title	Name of a method, framework, or model
Executive Summary	Structural abstract, context, objectives, approaches, findings, and conclusions
Review Questions	Specify each question
Review Methods	Data sources and search strategy, study selection, study quality assessment, data extraction, and data synthesis
Discussion	Primary findings, strengths, and weaknesses, and significance of findings
Results	Findings and sensitivity analysis

2.4 RISK-BASED STANDARDS

A risk is defined as a prospective occurrence that may result in the loss, damage, or destruction of an asset due to a threat exploiting a vulnerability, thus causing harm to an organisation. Risk is expressed as a function of two key factors: the probability of its occurrence and the magnitude of its impact or consequence.

On the other hand, risk management is a systematic process encompassing a series of activities aimed at proactively identifying and addressing risks. This process manages the risks of an organisation by establishing the risk context, identifying and assessing risks, reviewing them, applying appropriate measures of mitigation, and continuously monitoring risks to minimise potential threats and vulnerabilities, ultimately archiving acceptable levels of risk acceptance.

Furthermore, risk management consists of five key elements: asset, risk, threat, vulnerability, and control. Figure 2.6 represents the interlink between the risk management elements and how they form the risk management flow process.

The main purpose of an information security risk management process is to identify the risk event, estimate its consequences to the organisation, and then determine the likelihood that the identified event will occur. Furthermore, decision-makers (e.g., senior management/executives) need to assess the risk assessment outcomes. If the identified risks are not acceptable (e.g., based on the risk appetite matrix), then decision-makers should recommend a mitigation plan to further reduce risk (Wangen, 2017).

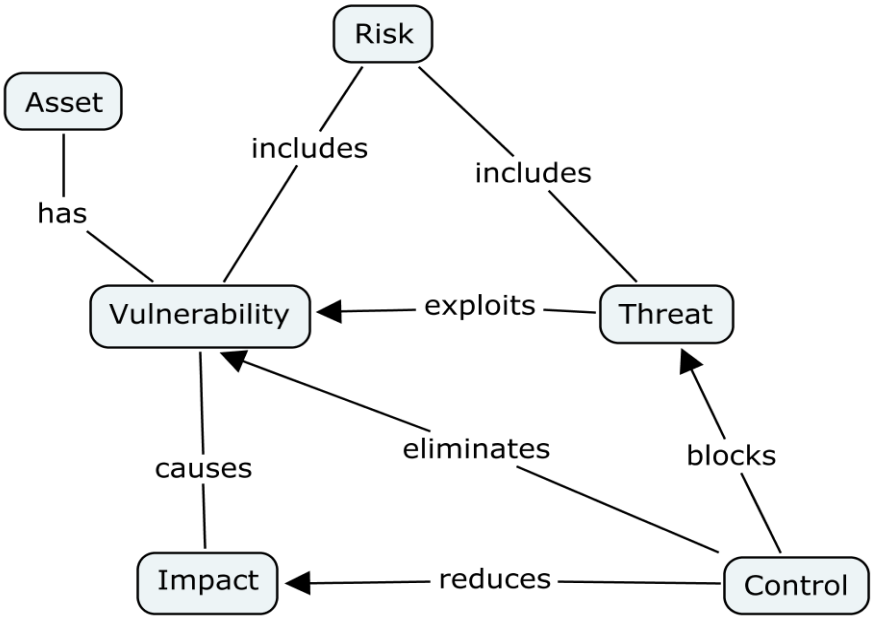


Figure 2.6: Risk Management Elements and their Interlink (Barateiro et al., 2012)

ISO (2022a) describes risk management as "coordinated activities to direct and control an organisation regarding risk". On the other hand, ISO (2018c) defines risk as "an effect of uncertainty on objectives, where the effect is a deviation from the expected". Risk can be positive, negative or both, and can address, create, and result in opportunities and threats. Objectives can have various aspects and categories and can be applied at various levels.

In general, risk is usually expressed in terms of four key elements: risk source, potential event, consequence, and likelihood, respectively. First, the risk source is defined as "an element which alone or in combination has the potential to give rise to risk". Second, the potential event is related to the occurrence or change of a certain set of circumstances. In other words, an event can have one or more occurrences and can have several causes and several consequences. Additionally, it can be a source of risk when something does not happen or when something unexpected does happen. Third, the outcome of an event affecting objectives is called a consequence. The consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. It also can be expressed qualitatively or quantitatively. Any consequence can escalate through cascading and cumulative effects. Forth, the last element is the likelihood in which a chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (e.g., a probability or a frequency over a given period) (ISO, 2018c).

2.4.1 Risk Management Evaluation Frameworks

The objective of risk management is to establish preventive and control measures to effectively mitigate the risks associated with specific activities and valuable assets. By promptly identifying potential risks, organisations can develop plans to minimise their potential impact (Barateiro et al., 2012).

Figure 2.7 describes the risk management elements and how they form the risk management flow process.

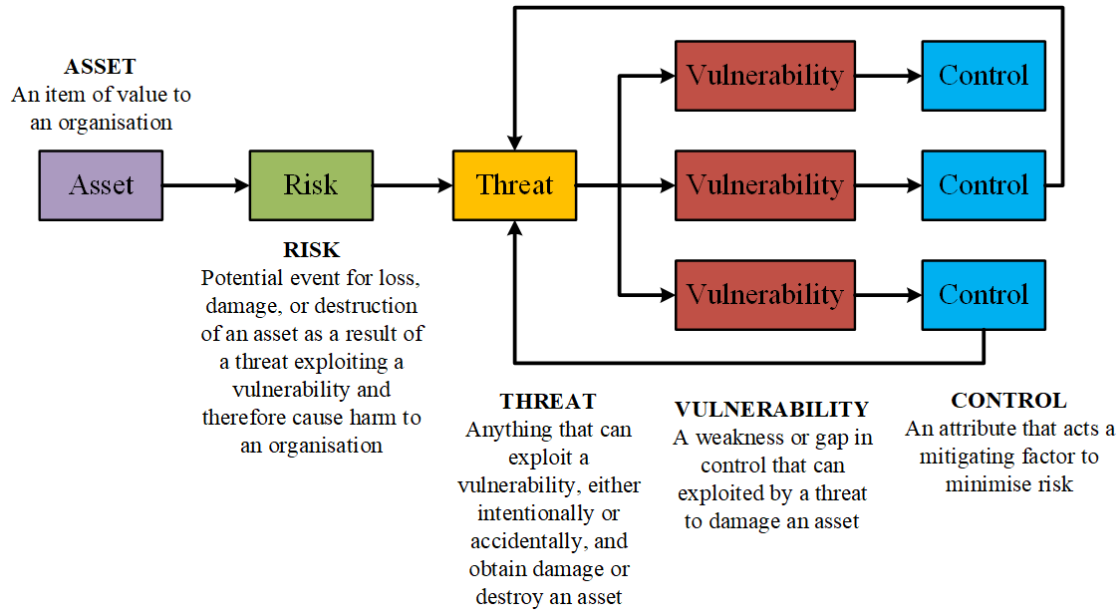


Figure 2.7: Risk Management Elements

There is a wide range of risk management frameworks relevant to IT and information security risk. For example, Vorster and Labuschagne (2005) proposed a framework to compare several information security risk analysis methodologies, including OCTAVE, Construct a Platform for Risk Analysis of Security Critical Systems (CORAS), Information Security Risk Analysis Method (ISRAM), Cost of Risk Analysis (CORA), and Information Security Risk Analysis Based on a Business Model (ISRAB-BM), using common criteria with a scaling level. These criteria address the following questions:

- Is risk analysis performed on a single asset or a groups of assets?
- At what point the methodology does risk analysis occur?
- Who are the stakeholders involved in the risk analysis activities (internal or external)?
- What type of formula is used to calculate risk (mathematical formula or

expected value matrix)?

- How are the methodology results related (relative or absolute)?

Syalim et al. (2009) conducted a comparative study on four risk analysis methods, including Mehari (2007), Magerit (2006), NIST 800-30, and Microsoft's security guide. Those methods were evaluated against two main criteria: risk assessment steps (e.g., threat identification, vulnerability identification, and risk determination), and method description and supporting documents (e.g., control recommendations catalogue). Shamala et al. (2013) suggested a conceptual framework of info-structure for Information Security Risk Assessment (ISRA) by comparing and analysing six risk methodologies, including CRAMM, CORAS, OCTAVE, ISRAM, ISRAB-BM, and NIST 800-30 in terms of four main characteristics (elements/features): management requirement, organisation context establishment, assets threats and vulnerabilities identification, and risk management improvement.

Agrawal (2015) presented a comparative study on four information security risk analysis methods, including CORAS, Conflicting Incentives Risk Analysis (CIRA), ISRAM, and ISRAB-BM based on eight criteria: methodology, purpose, input, effort, outcome, scalability, advantages, and weaknesses. The author concluded that each risk analysis method serves specific purposes. Thus, organisations need to define their needs first to choose a suitable framework solution for managing their potential risk. Wangen (2017) proposed an evaluation process in which a bottom-up approach is used. This approach determines cause-effect relationships between risk assessment methods and results. Additionally, it provides a way to evaluate several risk assessment methods by defining task sets or parameters as comparison criteria (i.e., assessment stages: risk identification, risk estimation, and risk evaluation). Three methods including OCTAVE A, ISO/IEC 27005, and NSMROS were evaluated and then scored for each identified task (i.e., 0 = not addressed, 1 = partially addressed, and 2 = fully addressed). The scoring process is a useful tool for determining which domains an organisation can expect all methods to perform well. The author also provided a high-level summary of the benefits and issues of each assessed method.

Selecting a framework is always a matter of organisation preference and what is required to fulfil an organisation's goals. Therefore, it can be used in a complementary approach with other frameworks, forming the base of a customised risk management framework (Almeida et al., 2019). The ISO/IEC 31000 standard has a risk management framework that gives complexity and description of how organisations can adapt it to

fulfil their requirements. Thus, Almeida et al. (2019) and Mayer et al. (2019) proposed a risk management model for ISO/IEC 31000 standard based on ArchiMate concepts and the Enterprise Architecture (EA) tool. However, in (Mayer et al., 2019) the scope was wider in which four EA references were considered: ArchiMate, The Open Group Architecture Framework (TOGAF), the Department of Defense Architecture Framework (DoDAF), and the Integrated Architecture Framework (IAF). The study by (Almeida et al., 2019) focused on six key principles: applicability to an organisation, a descriptive language for EA, economic restrictions, relevant components, systemic design, and comparability of different versions as well as three guidelines: objects structuring, a mapping between the ISO/IEC 31000 standard and the proposed model, and the relevant relations. On the other hand, Mayer et al. (2019) designed a new integrated EA Information System Security Risk Management (ISSRM) model. It was improved through two important aspects. First, it introduces constraints and stakeholders (which were not addressed in the current ISSRM model). Second, it defines a linkage between the business assets and the information security assets. The authors evaluated the usability of their proposed model using five main criteria: easy to learn, efficient to use, easy to remember, low-rate error, and satisfaction. Maneerattanasak and Wongpinunwatana (2017) reviewed the principles structure of five risk management frameworks, including Basel, ISO/IEC 31000 standard, ISO/IEC 27005 standard, COSO, and COBIT. They set eight processes: context setting, identification, analysis, evaluation, treatment, acceptance, monitoring, and communication; and then conducted content analysis against those frameworks to verify if their processes are fully addressed. Finally, the authors proposed a framework that presents the success factors for the adoption of principles and practices in implementing an IT risk management methodology.

Some risk management frameworks were designed for specific industry requirements such as telecommunications service providers (Mayer & Aubert, 2020) and SCADA systems (Cherdantseva et al., 2016). Hence, the task to set criteria or common properties for selecting a fit-for-purpose risk management methodology from a range of choices is possible for specific contexts. Since this research focuses on literature that is relevant to information security, five leading risk management frameworks have been chosen in the context of information security as follows:

- ISO/IEC 31000:2018 Standard
- ISO/IEC 27005:2022 Standard
- NIST Risk Management

- ENISA Risk Management
- The Risk IT Framework

Key elements of the candidate frameworks are summarised in the subsections below. Each of those frameworks has been developed to fulfil certain requirements and therefore has different objectives, structures, processes, and levels of application (Shamala et al., 2013). Moreover, each framework is described through various aspects, including the definition of risk used, its document structure, its main phases/processes, and the supporting security controls catalogue used where applicable.

2.4.2 Candidate Framework 1 – ISO/IEC 31000:2018 Standard

ISO/IEC 31000 standard defines risk as an effect of uncertainty on objectives. The effect is a deviation from the expected that can be positive, negative or both, and can address, create, or result in opportunities or threats. On the other hand, the objectives can have different aspects and categories; and can be applied at different levels. Overall, the risk is usually expressed in terms of sources, potential events, their consequences, and their likelihood (ISO, 2018c, 2022a). Risk management involves coordinating activities to direct and control an organisation regarding risk as defined in the ISO/IEC 31000 standard and ISO/IEC 27005 standard (ISO, 2018c, 2022a).

The second edition of the ISO/IEC 31000 standard was published in early 2018. This standard provides guidelines and common methods for managing any type of risk regardless of organisation size and type (i.e., not industry or sector-specific). Furthermore, it consists of three key components: principles (Clause 4), framework (Clause 5), and process (Clause 6) that work together to form a model to manage risk in an efficient, effective, and consistent manner as depicted in Figure B1.1, Figure B1.2, and Figure B1.3 respectively in Appendix B1.

Principles provide foundation and guidance on the aspects of managing risk in organisations. The ISO/IEC 31000 standard sets eight key principles that aim to ensure an organisation can create and protect its value as well as improve its performance, promote innovation, and support the achievement of the organisations' objectives. This framework aims to help an organisation integrate risk management into significant activities and functions. Framework development comprises five main elements: integration, design, implementation, evaluation, and improvement of risk management across the entire organisation.

The process consists of a set of policies, procedures, and practices for the various activities, including communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk. The IEC 31010 is a supportive standard that provides a set of techniques to help improve the risk assessment steps in a wide range of circumstances (i.e., identification, analysis, and evaluation) within the ISO/IEC 31000 framework. The risk assessment techniques can be applied within this structured approach (ISO, 2019).

Figure B1.4 in Appendix B1 shows examples of where within the ISO/IEC 31000 process techniques can be applied in an iterative approach to the various stages of risk assessment. This process also provides input into decisions about whether treatment is required, priorities for treatment and the actions planned to remediate risk (ISO, 2019).

ISO/IEC 31000 standard has perceived complexities and limitations in the description of how organisations can adapt it to fulfil their requirements. Although the ISO/IEC 31000 framework has effectively integrated the principles and process, it does not address how this framework will be integrated into an organisation's strategy. The ISO/IEC 31000 framework is seen as a practice-based approach, not an end-to-end framework that has specific requirements from an internal and external organisational environment (Lalonde & Boiral, 2012). Thus, it does not address any security controls that can be selected to mitigate the identified risks.

2.4.3 Candidate Framework 2 – ISO/IEC 27005:2022 Standard

ISO/IEC 27005 standard defines risk as an effect of uncertainty on objectives (the exact definition as in the ISO/IEC 31000 standard). It also provides more explanation about uncertainty and focuses on information security risk. It defines uncertainty as the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequences, or likelihood. The information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated likelihood of occurrence. Moreover, it is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation (ISO, 2022a).

The fourth edition of the ISO/IEC 27005 standard was published in October 2022. This standard provides guidelines and process steps for risk management framework in the context of information security to support organisations in implementing the Information Security Management System (ISMS) requirements (per ISO/IEC 27001:2022 standard). However, it does not provide any specific method for risk

management. Instead, organisations need to define their approach to risk management based on the scope of the ISMS, the context of risk management, and their business type (e.g., financial, telecommunication, IT, and manufacturing) (ISO, 2022a).

This standard is structured into three main parts: four introductory clauses (Clause 1 - 4), six core clauses (Clause 5 - 10) and an informative Annex. The introductory clauses describe the scope of the standard (Clause 1), the definitional reference ISO/IEC 27000 (Clause 2), the terms and definitions in the risk contexts based on the ISO/IEC 27000 (Clause 3) and then an overview of the structure of the ISO/IEC 27005 international standard (Clause 4).

On the other hand, the core clauses (Clause 5 - 10) define various activities of information security risk management as follows:

- A high-level description of the risk management process steps (Clause 5).
- The risk management context establishment with some details around the risk management approach (e.g., criteria of risk evaluation, impact, and risk acceptance), scope, and roles and responsibilities (Clause 6).
- The risk assessment activities (input, action, implementation guidance, and output) include the identification of risk, assets, threats, existing controls, vulnerabilities, and impact; risk analysis methodology and determination (likelihood and impact); and risk evaluation criteria (Clause 7).
- The risk treatment process activities and risk appetite include risk treatment, acceptance, avoidance, and transfer (Clause 8).
- The risk operation (Clause 9).
- Guidance on how to leverage related ISMS processes in the risk activities, including risk management communication, monitoring, review, corrective action, and improvement activities (Clause 10).

The last part of this standard is an informative annexe that presents some examples of practical techniques that could be used to support the risk assessment process such as the risk assessment approach (qualitative and quantitative) and risk components (e.g., incidents, risk resources, threats, vulnerabilities, consequences, and risk scenarios). Figure B2.1 in Appendix B2 shows the risk management process framework according to the ISO/IEC 27005 standard.

Context establishment is the first phase in risk management that aims to identify the scope, boundaries, and risk appetite an organisation is willing to accept. It defines the criteria necessary for risk management, including the impact of specific risks to an

organisation (e.g., disruption, damage to reputation, financial loss, and breaches of legal requirements) and an acceptable level of risk to an organisation based on various considerations (e.g., business, legal, operations, technology, and financial).

Several aspects that could cause a potential loss to an organisation (i.e., how, where, and why a loss might happen), are defined in the risk identification phase. These aspects include assets (e.g., information, processes, hardware, software, network, personnel, and site), threats (fire, flood, disclosure, software malfunction, unauthorised access, and theft of equipment), vulnerabilities (e.g., lack of audit trail, poor password management, and single point of failure), and impact (e.g., data breach, violation of legal obligations, and cost of interrupted operations).

The risk analysis phase determines the impact of the risk (i.e., incident scenarios), its likelihood, and then the level of risk (i.e., a combination between the impact and likelihood). The risk analysis can be performed using either a qualitative (based on subjective measurements e.g., Low, Medium, and High), a quantitative methodology (i.e., relying on absolute measurements such as mathematical calculation), or a combination of qualitative and quantitative methodologies. Then, the risk evaluation phase follows the risk analysis in which each level of risk is compared (i.e., as determined in the risk analysis phase) against the risk acceptance criteria (i.e., established in the context establishment phase). This is followed by prioritising the list of risks and developing plans to address them.

The risk treatment phase focuses on selecting appropriate controls to reduce the identified risk and then defining the risk treatment plan. The risk appetite has four options: treat, accept, avoid, and transfer as described in Table B2.1 in Appendix B2. Then, risk acceptance comes after defining the risk treatment plan. It involves making decisions about the identified risk based on the four options described in the risk treatment phase while considering the organisation's objectives. When an organisation selects an appropriate risk appetite, the risk communication and consultation phase begins, which involves discussing and establishing an agreement between decision-makers and other key stakeholders on how the risks should be managed and governed.

Lastly, the risk monitoring and review phase takes place to discover any changes in the context of an organisation and sustain a comprehensive assessment of the overall risk status on an ongoing basis. Furthermore, this phase aims to improve the current risk assessment activities as necessary and appropriate to an organisation's circumstances. ISO (2022a) recommends using the ISO/IEC 27001:2022 standard to select a set of

security controls. These controls are structured into four groups (families) as listed in Table B2.2 in Appendix B2.

2.4.4 Candidate Framework 3 – NIST 800-32 Risk Management

The National Institute of Standards and Technology (NIST) defines risk as a measure of the extent to which an entity is threatened by a potential circumstance or event. It is typically a function of two aspects: the adverse impact, or magnitude of the harm, that would arise if the circumstance or event occurrence; and the likelihood of occurrence (NIST, 2018).

NIST defines risk management as the program and supporting processes to manage risk to organisation assets, including mission, functions, image, and reputation. It also establishes the context for risk-related activities, including assessing risk, responding to risk once determined, and monitoring risk over time (NIST, 2018).

In December 2018, NIST published the second revision of the Risk Management Framework (RMF) (NIST, 2018). The RMF provides a set of guidelines for implementing the risk management framework in IS and organisations. It is a holistic, comprehensive, and flexible risk management process approach for effectively managing security and privacy risks in different environments. The RMF simplifies risk management activities execution (e.g., security categorisation, control selection, risk assessment, and monitoring) through automation processes and novel approaches for managing risk. It is a threat-centric method that does not address asset identification and evaluation, as well as stakeholder assessments. Instead, it allows for the use of subjective knowledge-based estimations, frequentist probability estimations, or a combination of them (Wangen et al., 2018).

The RMF is structured into four main parts: introductory, fundamentals, process, and eight supporting appendices. The introductory part highlights the importance and necessity of managing security and privacy risk from an organisational perspective. It also describes the key objectives of the RFM, its applicability, and its target audience. A high-level description of concepts for managing security and privacy risk is covered in the fundamentals part. This part also addresses the relationship between security and privacy programs in the RMF context. In contrast, the process part focuses on managing security and privacy risk through the implementation of various phases and their 47 associated tasks across all phases.

The last part of the RMF consists of eight supporting appendices. They offer supplementary information and instructions for executing the RMF, which includes a list

of relevant references such as standards, regulations and laws (Appendix A), common terms and definitions (Appendix B), common abbreviations used throughout the standard (Appendix C), detailed description of the roles and responsibilities of the interested parties involved in the risk management process (Appendix D), a summary of the RMF tasks with their associated primary responsibilities and supporting roles (Appendix E), system and common control authorisations processes (Appendix F), considerations for defining authorisation boundaries (Appendix G), and other considerations affecting the RFM execution (Appendix H).

Figure B3.1 in Appendix B3 shows the risk management process framework according to NIST (2018). The framework embodies a holistic and all-encompassing risk management process that incorporates the RFM into the System Development Lifecycle (SDLC). It consists of seven main phases (processes) with a set of tasks for each phase.

Organisational preparation is the first phase which looks at the RMF from both an organizational and a system-level viewpoint. This phase focuses on establishing a framework and priorities for effectively managing security and privacy risk within the organisation. Then, the system categorisation phase is employed to determine the criticality of the organisation's assets (information and system) based on the organisation's mission, business functions, and system functionality. When the organisation's assets are defined, a control selection is the next phase. An organisation starts choosing an initial set of controls based on asset categorisation. Thus, tailoring the selected controls as needed to minimise the identified risk to an acceptable level. Those selected controls are then implemented in the form of security and privacy plans.

Next, the controls assessment phase comes after deploying controls. The purpose of this assessment is to verify the effectiveness of the selected controls. The assessment checks if those controls are correctly implemented, functioning as intended, and producing the expected outcomes (i.e., using a proper procedure for assessing controls' effectiveness) as per the security and privacy requirements. Then, the controls assessment results are examined by a senior management/executive to decide whether the risk is acceptable or not.

The last phase of the RFM is to continuously monitor the implemented controls for any changes that might impact them. This encompasses evaluating the effectiveness of controls, documenting and modifications to the system and operational environment, performing risk assessments and impact analyses, and reporting on the security and privacy status of the system. Moreover, this phase incorporates all monitoring activities

(e.g., risk management, configuration management, and control effectiveness) into an integrated organisation-wide monitoring program. NIST (2020) defines a set of security controls baseline that could be appropriately tailored to the organisation's business needs and security requirements. In general, it consists of 20 security and privacy control domains (families) as presented in Table B3.1 in Appendix B3.

Each security and privacy family consists of a set of security and privacy controls for a baseline. Each baseline control set has a typical structure: a base control, discussion, associated controls, control enhancements, and references. Figure B3.2 in Appendix B3 shows an example of a typical control structure.

2.4.5 Candidate Framework 4 – ENISA Risk Management

ENISA defines risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation (ENISA, 2006). This definition is similar to the ISO/IEC 27005 definition. The ENISA defines risk management as a process of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options (ENISA, 2006).

The ENISA Risk Management Framework (ERMF) was published in June 2006 by the ENISA risk management/risk assessment working group (ENISA, 2006). This framework was developed based on two standards: OCTAVE and ISO/IEC 13335-2:1997 standard. The ERMF documentation is structured into various parts. The introduction is the first part that identifies four key issues that the proposed risk management framework should address, including the lack of awareness, absence of a common language, lack of feasibility studies of risk management methods and tools, and the lack of integration between risk management and organisational governance. A set of risk management implementation principles are discussed with a high-level description of five main processes and their associated activities. Moreover, the ERMF provides a high-level description of 13 distinct risk management methods (e.g., ISO/IEC 27005, OCTAVE, IT-Grundschutz and NIST SP 800-30) and has a list of 12 various risk management tools (e.g., COBRA, CRAMM, OCTAVE and RiskWatch).

The RFMF has six supporting annexes, including a list of terms and definitions, a template structure for risk management methods description with various attributes (e.g., lifecycle, licence, regulatory compliance, and geographical spread), a detailed description of risk management methods based on the template, a template structure for risk management tools description with various attributes, detailed description of risk

management tools based on the template and structure used for the work on risk management at ENISA. Figure B4.1 in Appendix B4 shows a schematic overview of the ERMF discussed here.

The ERMF is considered an umbrella under five phases (including one optional phase) and activities relevant to the identification, treatment, management, and control of risks take place. It starts with the risk management strategy phase that intends to incorporate all adopted risk management processes, activities, and methodologies. It consists of several activities including communicating and creating awareness of organisation risks (i.e., during and after treating risk), defining the risk management scope (e.g., the regulatory environment, internal and external stakeholders, business drivers, organisation culture, resources, and objectives) and establishing the risk management framework (i.e., goals and objectives, project activities, roles and responsibilities, and risk criteria).

Once the strategy has been defined, the risk assessment phase begins. The assessment comprises three main tasks: identifying threats, vulnerabilities, and their associated risks, assessing the level of the risks and their nature (i.e., estimating the impact and likelihood), and evaluating risks (i.e., deciding on treatment options). Then, planning a risk treatment comes after assessing the risk. In this phase, various activities are performed such as identifying security control options (e.g., transferring, avoiding, optimising, or retaining risk), developing a treatment plan, and then implementing those controls. Then after implementing the treatment plan, it is important to identify the residual risks (i.e., unidentified risks and untreated risks).

Risk acceptance is an optional phase in which senior management needs to decide either to accept, transfer, avoid, optimise, or retain the risk based on the defined risk criteria (in the first phase). This phase becomes optional because it can be embedded within the first and third phases. To ensure a continual improvement of risk management, the risk monitoring and review phase takes place at the end of the ERMF framework. The main purpose of this phase is to perform ongoing monitoring and review of risk management activities. The review measures the efficiency and effectiveness of the risk management processes, verifies the ongoing relevance and updates of the agreed treatment action plan, and re-assess the extent and compliance of management decisions. ENISA (2007) proposes a set of security controls grouped into two categories: organisational controls and asset-based controls. Table B4.1 in Appendix B4 lists two main security categories and their associated families.

2.4.6 Candidate Framework 5 – The Risk IT Management

The Risk IT defines two terms related to risk: business risk and IT risk. The business risk is a probable situation with uncertain frequency and magnitude of loss (or gain) while the IT risk is the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise (ISACA, 2009a).

Risk IT defines risk Management as a set of activities that assesses, controls, exploits, finances, and monitors risk from all sources to increase the organisation's value to its stakeholders (ISACA, 2009a). The Risk IT framework was published in 2009 by Information Systems Audit and Control Association (ISACA) that provides a set of enterprise risk management principles for organisations to effectively identify, govern, and manage IT risk. It is based on COSO and ISO/IEC 31000 risk management frameworks (ISACA, 2009a). It is also a high-level business-centric method that covers business aspects such as key risk indicators. Moreover, it provides a variety of tools and descriptions that could be used in conducting a risk assessment. It focuses on the creation of risk scenarios that include the definition of actors, threat type, event, asset/resource, and time. The Risk IT framework supports both frequency and qualitative assessments or a combination of them. However, it does not address tasks/activities related to threat and control assessment as part of the risk identification process (Wangen et al., 2018).

In general, Risk IT primarily addresses IT components that align with various enterprise risk standards spanning multiple domains. Additionally, it aligns with established frameworks such as COBIT and Value Information Technology (Val IT), which serves as overarching structures for managing risk within other specialised IT framework, practices, and process models like ISO/IEC 27001, Information Security Framework (ISF), and Information Technology Infrastructure Library (ITIL). The Risk IT defines six key principles for effective management of IT risk. It is structured in five main parts: introduction, principles, framework, process model, and supporting appendices as illustrated in Figure B5.1 in Appendix B5.

The framework starts with an introduction that provides a high-level executive summary of the Risk IT (e.g., the relationship between Risk IT, COBIT, and Val IT), its objectives, and its intended audiences and stakeholders. Then, the second part defines and explains in detail six principles of the framework, including the business objectives linkage, risk management alignment, cost and benefit balance, risk communication and promotion, accountability establishment, and risk management as part of daily activities. The high-level description of the Risk IT framework phases (governance, evaluation, and

response) and their relevant components are covered in the third part. The detailed process model is further explained in the fourth part. It also describes the main goal, key activities, inputs, and outputs for each process. Moreover, it provides a foundation to create a maturity model that could be used for process evaluation.

The last part is dedicated to supporting appendices. This part provides a list of references with guidance on how to develop the framework (Appendix 1) and compares the Risk IT with six other frameworks, including COSO, ISO/IEC 31000:2009, AS/NZS 4369:2004, AIRMIC, ISO/IEC 2000-1/2:2005 and ISO/IEC 27005:2008, ISO/IEC 27001/2:2005 (Appendix 2), and describes the relevant terms and definitions (Appendix 3). The Risk IT framework consists of three main phases, each containing three key activities as depicted in Figure B5.2 in Appendix B5.

The framework starts with the risk governance phase that embeds IT risk management activities into the organisation. This phase includes various activities such as adapting IT risk practices, defining risk appetite and tolerance thresholds, assigning roles and responsibilities, communicating, and promoting the risk management activities to organisation stakeholders and ensuring the risk is understood and maintained within the organisation. Secondly, risk evaluation starts after completing the risk governance phase. The evaluation aims to define, analyse, and present IT risks and opportunities. This phase involves several activities such as collecting information about the organisation's environment and risk events, defining IT risk scenario components (e.g., event, threat type, asset, stakeholders, and timing), estimating occurrence and business impact, and then establishing a risk profile.

The last phase of the Risk IT framework is to respond to risk to identify IT risk issues, opportunities, and events based on organisation priorities. Activities are executed as part of this phase, including defining key risk metrics, defining risk response options (avoidance, reduction/mitigation, sharing / transfer, and acceptance), selecting and prioritising the appropriate option based on numerous factors (e.g., cost, importance, implementation capabilities, response effectiveness and efficiency), and then implementing controls. The Risk IT Practitioner Guide (ISACA, 2009b) plays a significant role in supporting the Risk IT framework implementation. This guide provides a security controls catalogue (based on IT risk scenarios and environmental risk factors) mapped to COBIT 2019 and the Val IT framework. It also lists various scenarios and their associated controls. All of these elements also transfer into the COBIT 2019 framework.

57 controls are chosen that are aligned with the information security context; and grouped into 12 families as defined in Table B5.1 in Appendix B5.

2.4.7 Comparison of Risk Management Frameworks

To compare and analyse the selected risk management frameworks: ISO/IEC 31000, ISO/IEC 27005, NIST, ENISA, and The Risk IT discussed previously, a systematic method has been followed:

- Identification of risk-based activities in all the frameworks.
- Creation of a list of artefacts created, developed, and extracted as outputs in all the frameworks.
- Mapping of the listed artefacts to all the frameworks.

Table 2.3 provides a list of artefacts created, developed, and extracted as outputs from the selected frameworks. Although ENISA does not explicitly list the expected outcomes of the ERMF, the artefacts presented in Table 2.3 were extracted from the ERMF description. NIST is the only framework that addresses privacy in various areas (e.g., requirements, control plans, control catalogues, and assessment reports) as part of the overall risk management framework.

Table 2.3: Artefact Baseline Mapping for the Selected Frameworks (ISO/IEC 27005, NIST, ENISA and The Risk IT)

Artefacts	ISO31000	ISO27005	NIST	ENISA	The Risk IT
Scope and Boundaries	☑	☑		☑	☑
Risk Assessment Criteria	☑	☑			
Roles and Responsibilities	☑	☑	☑	☑	☑
Internal, External and System Stakeholders	☑	☑	☑	☑	
Risk Assessment Tool			☑		
Business Requirements				☑	☑
Security and Privacy Requirements			☑		
Risk Management Strategy			☑		
Information Lifecycle[1]			☑		
External Audit Findings					☑
Risk Management Policy				☑	☑
Project Plan				☑	
Communication / Awareness Plan				☑	☑

Artefacts	ISO31000	ISO27005	NIST	ENISA	The Risk IT
Risk Treatment / Remediation Plan[2]	☑	☑	☑	☑	☑
System Description			☑		
Asset / Resource Inventory	☑	☑	☑		☑
Business Processes		☑			
Risk Assessment Reports / Risk Analysis Results	☑	☑	☑		☑
Security and Privacy Posture Reports			☑		
Key Risk Indicators (KRI)					☑
Controls Validation Report			☑		
Security and Privacy Assessment Reports			☑		
Assessors / Assessment Team			☑		
Security Controls Catalogue[4]			☑		
Privacy Controls Catalogue			☑		
Selected Security Controls[4]			☑		
Tailored Control Baselines			☑		
Risk Profile[3]	☑	☑	☑	☑	☑
Risk Prioritisation		☑			
Incident Scenarios		☑			
Risk Evaluation Criteria	☑	☑		☑	
Risk Treatment Effectiveness				☑	
Risk Acceptance Criteria	☑	☑			
System Security and Privacy Plans			☑		
Organisation System Prioritisations			☑		
System Components Inventory			☑		
Common Control Providers			☑		
Authorisation Boundary			☑		
System Information Types			☑		

[1] *E.g., data flow diagrams, entity, relationship diagrams, database schemes and data dictionaries*.

[2] *Existing controls, planned controls, and their implementation status.*

[3] *Risk issues, risk opportunities, risk scenarios, impact assessment, vulnerabilities, threats and their sources.*

[4] *ISO/IEC 27005:2022 refers to the ISO/IEC 27002:2022 as the security controls catalogue.*

2.5 ELEMENTS OF ISO/IEC 27050 STANDARD

ISO/IEC 27050 eDiscovery standards offer a best practices framework for investigations, evidence acquisition, and handling activities. The framework describes the necessary rules and steps to identify and preserve the relevant ESI (i.e., when an investigation is initiated) to meet jurisdictions, courts, and regulation requirements (e.g., civil, and criminal proceedings, investigations, and audits purposes). The ISO/IEC 27050 series standard is structured into four parts as described in Table B6.1 in Appendix B6.

The ISO/IEC 27050 standard identifies and refers to other relevant ISO standards and how they relate to and interact with eDiscovery activities. These include, but are not limited to (ISO, 2018a):

- **ISO/IEC 27000** – Applicable terms and definitions in the context of an ISMS.
- **ISO/IEC 27037** – Specific activities in identifying, collecting, acquiring, and preserving digital evidence.
- **ISO/IEC 38500** – Governance principles on the effective, efficient, and acceptable use of IT.
- **ISO/IEC 27040** – Guidance for defining risk mitigation of data storage security.

The identification and preservation of ESI are essential for various purposes. These include anticipating potential legal actions, receiving a pre-litigation preservation request, responding to inspection requests, addressing demand letters, cease-and-desist letters, cure notices, or even engaging in discussions with a third party.

ESI can be found in a wider range data of sources classified into two types:

1. **Custodian Data Sources** – Under direct control of a custodian (e.g., desktops, laptops, and removable storage media such as thumb drives, external hard drives, DVDs, or CDs).
2. **Non-Custodian** – Not under the control of a custodian (e.g., databases, application, NAS, SAN, backup tapes, digital archives, cloud storage and social media).

Moreover, the ISO/IEC 27050 standard is designed to align with jurisdictional laws and regulations, rather than contradict or override them. Its primary objective is to facilitate ESI investigations, evidence acquisition, and handling processes (Bhatia & Malhotra, 2020).

From a governance perspective, the ISO/IEC 27050 standard uses ISO/IEC 30121 standard as a risk governance framework reference from a digital forensics perspective. The ISO/IEC 30121 standard supplies a framework for governing bodies of organisations (e.g., owners, management teams, and partners) on how to prepare an organisation for digital investigations before they happen. It also sets an elevated-level governance framework that consists of six processes: information archiving and retention, eDiscovery, information disclosure, digital evidence prevention, risk mitigation strategy, and risk monitoring and reporting process as depicted in Figure B6.1 in Appendix B6 (ISO, 2016, 2018b).

The eDiscovery is a systematic process that involves seven main phases: identification, preservation, collection, processing, reviewing, analysis, and production. Figure 2.8 depicts the interrelationship between the seven eDiscovery phases. The analysis phase is placed in the outer circle because it is considered an optional phase (e.g., the identification process might require an analysis to be performed and then the process flow returns to back to the identification for an additional activity). The process flow moves from one phase, other than the analysis phase, to another and then returns to the previous phase. Furthermore, Figure 2.8 shows circular arrows which means that the eDiscovery phases can be executed in a sequence and iterative manner.

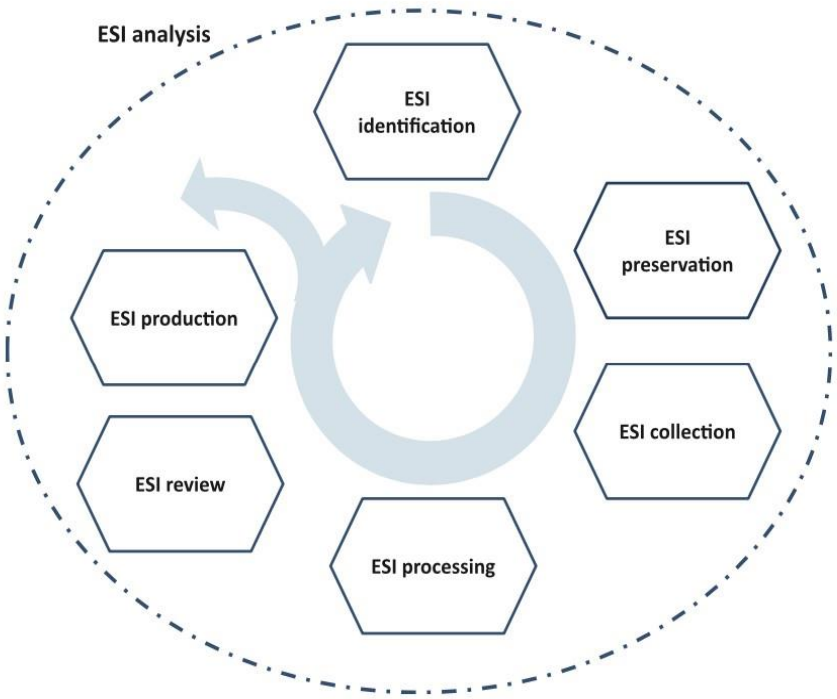


Figure 2.8: Electronic Discovery Process Lifecycle (ISO, 2018a, p. 16)

The subsections below describe the eDiscovery phases in more detail.

2.5.1 Phase 1 – Identification

The identification phase allows understanding the relevant subject matter, such as anticipating potential litigation, receiving pre-litigation preservation requests, examining requests, demands, cease-and-desist letters, cure notices, or engaging in discussion with opposing parties or their legal representatives. Moreover, this phase aims to identify key personnel (e.g., departments, individuals, and custodians) involved in the eDiscovery activities, ESI data types (e.g., active, inactive, residual, and legacy), ESI locations, and ESI sources that could potentially uncover relevant information on a specific subject matter (ISO, 2018a, 2020a, 2020b).

2.5.2 Phase 2 – Preservation

The preservation phase ensures that necessary steps based on authority obligations are taken to keep the identified electronic information from any potential modification, destruction, or inaccessibility. In other words, the essential objective of this phase is to perform preservation with a reasonable level of completeness and accuracy at a reasonable expenditure of time and resources (ISO, 2018a, 2020a, 2020b). The preservation can be achieved by various methods, including coping the identified electronic information directly from its source, and safekeeping of the identified electronic information where it normally stores either through custodian self-preservation or in-place preservation using appropriate technologies.

2.5.3 Phase 3 – Collection

The collection phase is a copying practice in which copies or images of the preserved information (i.e., target files) are obtained and included in a data set (i.e., created from hardcopy documents and ESI) that can then be passed on to downstream processing and review (ISO, 2018a, 2020a, 2020b). Several tools and methods can be used for collection purposes depending on various instances such as device types (e.g., a desktop computer vs a smartphone), file types (e.g., email vs a microblog post), law streams (e.g., criminal vs civil) and authority requirements (how the investigation is conducted).

2.5.4 Phase 4 – Processing

The processing phase aims to ensure that the required measures are implemented to reduce the data volumes (using various filtering techniques) by removing out-of-interest files, so the filtered data can be easily searchable and presentable in a reviewable format (ISO, 2018a, 2020a, 2020b). ESI can be collected in various formats that need to be held

for further processing (i.e., cataloguing and capturing), including individual files, e-mail extracted from container files (e.g., PST, NSF, ZIP, RAR, etc.), and certain types of ESI (e.g., legacy e-mail and legacy file). Furthermore, the processing phase is split into four main stages: assessment, preparation, selection, and output. It starts with the assessment stage to find if certain ESI does not need to move forward. Then, follows another stage to prepare the ESI for item-level selections to occur (i.e., extraction, indexing, hashing, etc.). The selection stage involves de-duplicating, searching, and analytical methods. It ends with the output stage to ensure secure transport of reviewable items is performed.

2.5.5 Phase 5 – Review

The review phase is a screening assessment in which the collected and processed hardcopy documents or ESI that meet the production criteria are separated from those that do not (ISO, 2018a, 2020a, 2020b). To accomplish an effective review, various methods must be considered such as the use of manual review, the use of technology-assisted review, and the use of combination methods which use both human review and automated tools.

2.5.6 Phase 6 – Analysis

The analysis phase aims to support and assist all iterative phases of the eDiscovery process (i.e., identification, preservation, collection, processing, review, and production); and increase the process efficiency. It takes an in-depth analysis of a document or ESI to determine its provenance using various analytics tools and methods (ISO, 2018a, 2020a, 2020b). Table B6.2 in Appendix B6 describes how the analytics are applied during the execution of the eDiscovery process (ISO, 2020a).

2.5.7 Phase 7 – Production

The production phase aims to prepare the agreed files to be delivered from a party to requesting parties (e.g., an external party or another internal team). In other words, the delivery is about producing the results of the review phase (ISO, 2018a, 2020a, 2020b). There is a set of aspects that need to be considered while preparing for ESI production, including file type format, file conversion requirements, metadata preservation, endorsement requirements, tooling and printing costs, and file transfer requirements.

Both the ESI presentation and the chain of custody are two more aspects that need to be considered during the execution of the eDiscovery process. They play a key role in presenting admissible ESI evidence in court (ISO, 2018a). The presentation ensures that

ESI exhibits in several formats: near-paper (e.g., files in the format they were created and kept such as spreadsheets and small databases), image or near-paper (e.g., converting ESI or scanning paper into a non-editable digital file), near-native (e.g., extracting and converting files into a generic format analysis such as emails and large databases), and hardcopy depending on legal requirements. Additionally, the chain of custody documents and tracks how the information associated with ESI is created, changed, transferred, and dispositioned. It is an essential aspect to show the ESI process quality, integrity, and authenticity in the courts.

2.6 UNIVERSITY RESEARCH ON STANDARDS

Standards play a significant role in setting up a shared framework for innovation, enhancing markets, and generating many opportunities. A standard is a document that servers as a reference point, offering comprehensive technical specifications, common vocabularies, and essential features of a product or service (Hoel & Chen, 2018; Shin et al., 2015). Hoel and Chen (2018) conducted a study that primarily explores ways to enhance the interaction between the research and the standardisation communities to effectively define requirements. Standardisation is a design activity that has a direct connection with innovation processes. The authors described a framework for standards-setting based on DSRM. The DSR activities are situated in one of four quadrants in the cross-section of solution maturity and application domain maturity.

The interaction between various stakeholders: the academic researchers, the standards practitioners, and the users of standards could attribute to the technical quality and the expected outcomes of the standard. The model in Figure 2.9 represents this integration through a series of activities. It starts by initiating a project and seeking input from academic researchers. The academic researchers work together with practitioners (implementers) to design and test standard artefacts through numerous iterations, and a final design for the developed standard (Hoel & Chen, 2018).

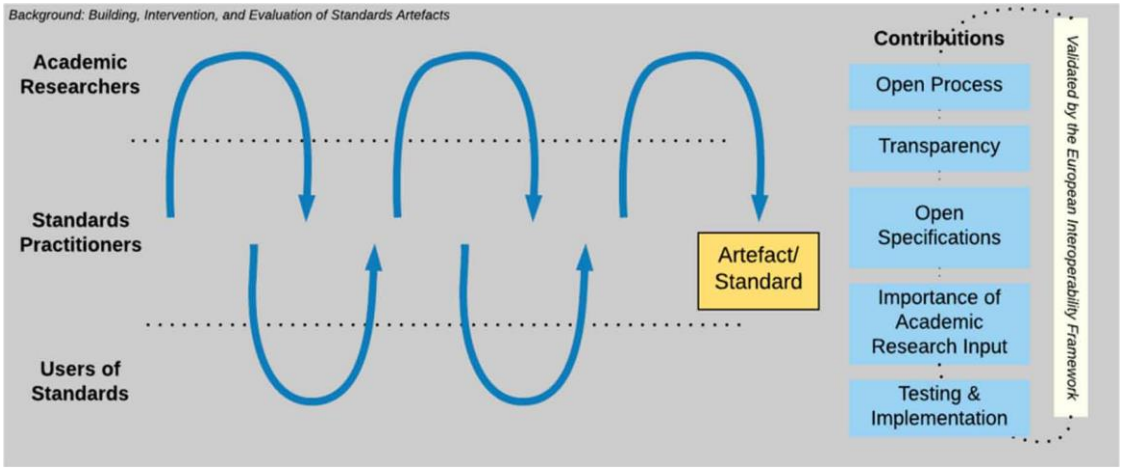


Figure 2.9: An Ideal Model of Standards-Setting Coming Out of the Background Research Contribution (Hoel & Chen, 2018, p. 27)

Participation in standardisation costs time and money. Thus, de Vries and Veurink (2017) introduce an innovative decision-making tool that could be used to evaluate the feasibility of contributing to a standardisation process. This tool consists of five stages in which standardisation can be assessed as follows:

- **Stage 1 – Project Description**: It provides essential details about the standardisation project and the parties involved.
- **Stage 2 – Qualitative Assessment**: It assesses the likelihood of success in two scenarios: if the organisation participates in the standardisation process and if it chooses not to participate. It then outlines the key advantages and disadvantages of investing in participation.
- **Stage 3 – Quantitative Assessment**: This evaluation measures the impact of the standard on revenues, costs, or relevant components. It encompasses important project parameters (e.g., the initial year, implementation year, impact calculation, corporate interest rate, losses due to delayed implementation, and annual standardisation costs).
- **Stage 4 – Financial Indicators**: Using both qualitative and quantitative input, this stage automatically generates and summarises the financial outcomes of the standardisation project.
- **Stage 5 – Advice**: Drawing upon the results in Stage 4, the standards professional can state the considerations during the project evaluation. The tool advises on whether participation in a standardisation project is recommended or not. If the tool is employed to evaluate past projects, it will generate a summary of success factors.

Many Information and Communications Technology (ICT) standards have emerged through collaborations among industry consortia and occasionally from individual organisations, unlike most other domains that rely on formal standards. However, as technologies like smart manufacturing or intelligent transport systems increasingly converge, the boundaries between ICT standards and those in other domains become less significant. The emergence of standards from various sources arises new questions about the consistency of the standards needed for a specific domain. This, in turn, impacts standardisation processes and the overall governance of standardisation (de Vries et al., 2018).

Standardisation research is conducted in several countries including China, the Republic of Korea, Japan, Northern and Western Europe, Canada, and the USA. While some researchers in developing countries and transitional economies also engage with standardisation, their focus tends to be more on teaching rather than research, and their work is seldom published in internationally recognised journals. Consequently, the significance of standards and standardisation in these countries receives limited attention in academic research. Moreover, the exploration of diverse standardisation practices, cultures, and institutions remains an area that is insufficiently investigated. There are notable differences in these aspects among regions such as Africa, Australia, Asian countries (e.g., China, Indonesia, and Japan), Europe, the Middle East, the Russian Federation, South America, and the USA all differ in these respects. Gathering research data to analyse such variations is challenging, as many standards bodies are not transparent when it comes to disclosing relevant details of actual standardisation projects, despite transparency being one of the principles outlined by the World Trade Organisation (WTO) (de Vries et al., 2018). A cohesive theoretical framework is required for the domain of standardisation, enabling a systematic understanding and acquisition of empirical evidence regarding current practices. To achieve this, it is necessary to conduct multi-method research, encompassing quantitative studies that rely on tangible data rather than subjective perceptions. To obtain such data, researchers should collaborate with organisations that process or have the capability to gather relevant information, such as standards bodies, statistical offices, and trade associations (de Vries et al., 2018).

Shin et al. (2015) conducted a study on the standardisation strategies framework from two different perspectives: demand and supply. The demand focuses on how organisations decide whether to stay with existing technology standards or adopt a new standard. On the other hand, the supply focuses on how organisations create a technology

standard and what types of technology standard processes are considered (e.g., government-led standard, the standard-setting process, market-based standardisation, committee-based standardisation, and consortium-led standardisation).

Blind and Gauch (2008) examined the common ground between formal standardisation bodies (e.g., BSI, ESOs, ISO, IEC, and ITU) and informal ones (e.g., IETF, W3C, and IEEE) in terms of ICT technical specifications. They analysed and compared the activities of standardisation processes between the bodies. Their study revealed a significant impact of technological trends (e.g., mobile communication, WAN, and ISDN) on the activities. These factors foster complementary relationships among different activities rather than substitutive relationships.

Recent research on adopting international standards was presented in (Li & Pang, 2020). They proposed four principles for any country's interest in developing its national standards based on international standards. Those principles include complying with relevant international standards rules and policy (i.e., ISO/IEC), adopting standardised documents (e.g., technical specifications and technical reports), ensuring the adoption does not affect the national standards and their acceptance, and finally incorporating all amendments and/or technical corrigendum into the national standards for integrity purposes. Furthermore, the authors made a comparative study between six major countries: Germany, the UK, the US, Japan, Russia, and China in terms of the rules and procedures used for adopting international standards and then integrating them into their national standards.

2.7 SUMMARY OF ISSUES AND PROBLEMS

Standardisation is an intensive process that requires time and investments to implement. The main purpose of a standard document is to create rules and guidelines for activities. A standard consists of three key aspects: science, technology, and experience. Furthermore, developing a standard involves a well-defined procedure starting from the proposal stage to the publication stage. Key points are summarised in the following sub-sections.

2.7.1 Summary

As discussed previously in Section 2.4, the risk management process can be described as coordinated activities to direct and control organisations with risk. This process consists of four main components: risk source, potential event, consequence, and likelihood. It is a complex task to set criteria for selecting a fit-for-purpose risk management methodology

from a range of frameworks. Table 2.4 provides a security comparison between the risk-based standards discussed in Section 2.4.2 to Section 2.4.7.

Table 2.4: Risk-Based Standards Comparison

Risk Standard	Developed by and Publication Date	Risk Method/Phases	Security Controls Baseline
ISO/IEC 31000	ISO in 2018	1. Scope, Context, and Criteria Definition 2. Risk Identification 3. Risk Analysis 4. Risk Evaluation 5. Risk Treatment 6. Risk Monitoring and Review 7. Risk Recording and Reporting	N/A
ISO/IEC 27005	ISO in 2022	1. Context Establishment 2. Risk Identification 3. Risk Analysis 4. Risk Evaluation 5. Risk Treatment 6. Risk Acceptance 7. Risk Communication and Consultation 8. Risk Monitoring and Review	ISO/IEC 27002:2022 (Annex A)
NIST 800-37	NIST in 2018	1. Organisational Preparation 2. System Categorisation 3. Controls Selection 4. Controls Implementation 5. Controls Assessment 6. System Authorisation 7. Controls Monitoring	NIST Special Publication 800-53 Revision 5
ENISA Risk Management	ENISA in 2006	1. Risk Management Strategy 2. Risk Assessment 3. Risk Treatment 4. Risk Acceptance 5. Risk Monitoring and Review	Selected Controls from OCTAVE

Risk Standard	Developed by and Publication Date	Risk Method/Phases	Security Controls Baseline
The Risk IT	ISACA in 2009	1. Risk Governance 2. Risk Evaluation 3. Risk Response	Risk IT Practitioner Guide

Based on the above comparative analyses, it can be concluded that the risk-based standards have common risk methods/phases such as identification, evaluation, and treatment but with different levels of detail. The goal of these models is to mitigate, transfer, accept, or reduce risks to an acceptable level by ranking and evaluating the risk value. Furthermore, each risk-based standard uses its security control catalogue depending on its area of focus (e.g., Annex A for ISO/IEC 27001 or IT controls for the Risk IT).

2.7.2 Gap Analysis

ISO/IEC 27050 series (especially Part 1 and Part 2) provide a set of guidelines on how to handle ESI and support eDiscovery through seven main processes: identification, preservation, collection, processing, review, analysis, and production (Arshad et al., 2020; Nieto et al., 2017). Additionally, the ISO/IEC 27050 standard provides a legal perspective as part of the eDiscovery lifecycle. It can be used for technical and non-technical aspects, but it focuses on the requirements for regulatory and industry standards. It provides recommendations on how to manage ownership of risks related to ESI (e.g., creating and implementing the required policies for compliance adherence) (Al-Khateeb et al., 2019).

Although ISO/IEC 27050 standard helps in identifying the risks associated with eDiscovery and then providing a basic mitigation plan, it does not provide a detailed description of how to perform risk analysis and manage the identified risks. Instead, it only provides high-level requirements for the whole ESI investigation process. The ISO/IEC 27050 uses ISO/IEC 30121 as the risk governance framework reference for a digital forensic process. The ISO/IEC 30121 suggests that an organisation should adopt a strategic risk (i.e., the effect of uncertainty on goals) framework for digital evidence to ensure that the level of risk remains within the organisation's risk criteria (ISO, 2016). However, the ISO/IEC 30121 does not provide a holistic approach to managing risk in

the digital forensic context. Instead, its primary emphasis lies in preparing an organisation for digital investigations in advance of their actual occurrence.

The elements (i.e., main phase and relevant activities) of the risk management reference model presented in Figure 2.10 were adapted and selected based on the analysis of three chosen frameworks including CURF (Wangen et al., 2018), ISRA (Shamala et al., 2013), and ISO/IEC 27005 (ISO, 2022a). They share the common four phases: context establishment, risk identification, risk estimation, and risk evaluation and treatment. A set of activities are identified in each phase (21 activities in total).

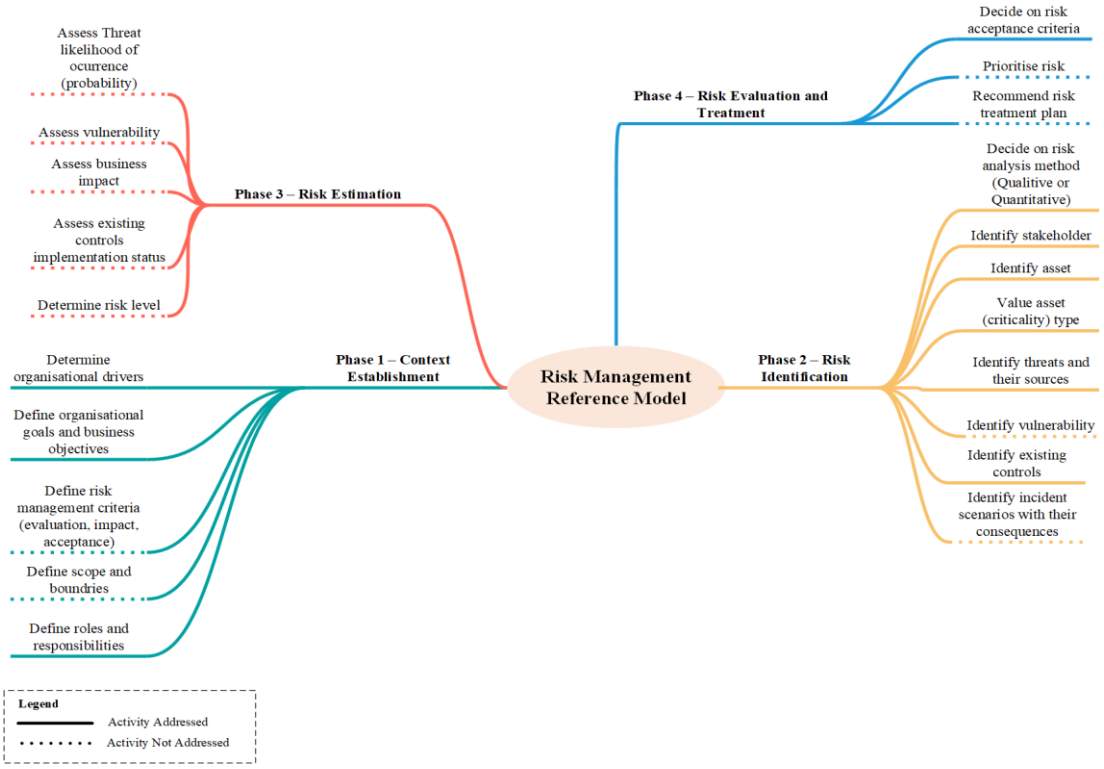


Figure 2.10: Elements of The Risk Management Reference Model (ISO, 2022a; Shamala et al., 2013; Wangen et al., 2018)

It has been observed that the ISO/IEC 27050 standard does not encompass all elements of the risk management reference model described in Table 2.5. The ISO/IEC 27050 is evaluated according to the following approach:

1. If an activity is addressed in the ISO/IEC 27050, then a mapping commentary is provided along with the exact reference (either ISO/IEC 27050-1, ISO/IEC 27050-2, ISO/IEC 27050-3, and/or ISO/IEC 27050-4) and location (page number).
2. If not addressed (i.e., presented in a dotted line in Figure 2.10), then no commentary is required.

In this way, the risk management phases are mapped with coherent activities and compared to show how they divert from the ISO/IEC 27050. Consequently, this approach allows the researcher to conduct a detailed qualitative comparison of activities between the risk management phases reference model and the ISO/IEC 27050.

As shown in Table 2.5, 50% of the risk management reference model activities (11 activities) are not addressed within the ISO/IEC 27050 which represents a significant gap. Furthermore, the entire Phase 3 (risk estimation) is missing from the ISO/IEC 27050 and most of Phase 4 activities (risk evaluation and treatment). Two activities of Phase 1 (context establishment) and Phase 2 (risk identification) are not covered.

Table 2.5: Reference Risk Management Phases Based on The Literature (ISO, 2018a, 2018b, 2020a, 2020b, 2022a; Shamala et al., 2013; Wangen, 2017; Wangen et al., 2018)

ID#	Activity	Observations / Gaps	Reference(s)
Phase 1 – Context Establishment			
1.1	Determine organisational drivers	The standard identifies the key drivers for establishing an ESI process. including compliance requirements (e.g., statutory, regulatory, and legal) (ISO, 2018b).	ISO/IEC 27050-2: page 7
1.2	Define organisational goals and business objectives	The standard highlights some essential elements for eDiscovery governance, including risk and environmental, compliance and review, and privacy and data protection (ISO, 2018a). Furthermore, the standard provides a list of goals that should be considered for the eDiscovery process (ISO, 2018b).	ISO/IEC 27050-1: page 8 ISO/IEC 27050-2: page 6
1.3	Define risk management criteria (evaluation, impact, acceptance)	Not addressed	N/A
1.4	Define scope and boundaries	Not addressed	N/A
1.5	Define roles and responsibilities	The standard proposes a list of roles and responsibilities (core team) for managing ESI, including an information security officer, senior manager, subject matter experts, counsel, eDiscovery lawyers, litigation support personnel, IT specialists, records manager and digital forensic experts. It is important to note that those roles might not be directly relevant to risk management (ISO, 2020b). Moreover, the standard also emphasises that an organisation needs to establish a project team. This team includes a project sponsor and manager from the business, legal and ICT teams (ISO, 2018a).	ISO/IEC 27050-4: pages 27-28 ISO/IEC 27050-1: page 9

ID#	Activity	Observations / Gaps	Reference(s)
Phase 2 – Risk Identification			
2.1	Decide on a risk analysis method (Qualitative or Quantitative)	Not addressed	N/A
2.2	Identify stakeholder	The standard suggests that an organisation needs to identify a team of key people for ESI discovery management, including corporate legal counsel, external legal advisors, ICT staff, records management personnel, data custodians, human resources personnel, business executives, and service providers or eDiscovery consultants (ISO, 2020a). Furthermore, the standard emphasises that an organisation needs to engage stakeholders as part of the ESI process, such as opposing counsel or the judicial decision maker in a litigation matter, or employees in an internal audit (ISO, 2020b).	ISO/IEC 27050-4: page 28 ISO/IEC 27050-3: page 5
2.3	Identify asset	The standard recommends, whenever feasible, before an actual eDiscovery incident, it is advisable to generate a catalogue of systems, or a data map, which would serve as a centralised listing outlining the various types of ESI possessed by the organisation and their respective storage locations (ISO, 2020a). The standard provides a list of potential ESI assets categorised into distinct types (ISO, 2018a, 2020a, 2020b): • Documents (e.g., email, memos, letters, spreadsheets, office documents, and presentations) • Data processing (e.g., computer, system, and application)	ISO/IEC 27050-1: pages 2,4,12,14,17,18 ISO/IEC 27050-3: page 6 ISO/IEC 27050-4: pages 6, 15, 22

ID#	Activity	Observations / Gaps	Reference(s)
		• Electronic medium (thumb drive, external hard drive, DVD or CD, and tape drive) • Mobile device (mobile phone, tablets, and GPS)	
2.4	Value asset (criticality) type	The standard suggests that an organisation should design a data map for each ESI item. The mapping will offer comprehensive information regarding potentially discoverable data repositories and the methods by which the data contained within them can be produced. Such insights will assist in making informed decisions during the selection process of the discovery system, considering factors related to data production (ISO, 2020b).	ISO/IEC 27050-4: pages 7, 22
2.5	Identify threats and their sources	The standard identifies the primary issues associated with ESI process elements as follows (ISO, 2020a): • Identification (e.g., destruction of ESI by runtime) • Preservation (e.g., Failure to recognise and respond to a triggering event) • Collection (e.g., file alteration) • Processing (e.g., inaccurate assessment) • Review (e.g., time overrun), • Analysis (e.g., in support of ESI preservation) • Production (e.g., inadvertently producing privileged, confidential, sensitive, or trade secret information)	ISO/IEC 27050-3: pages 4, 7, 11, 15, 18, 23, 21, 23
2.6	Identify vulnerability	Not addressed	N/A

ID#	Activity	Observations / Gaps	Reference(s)
2.7	Identify existing controls	The standard addresses that an organisation needs to set and implement control policies for the ESI process. These policies include archival policies (e.g., BCP, a chain of custody, retention period), discovery policies (e.g., discovery mechanisms), and disclosure policies (e.g., information disclosure criteria) (ISO, 2018b).	ISO/IEC 27050-2: pages 5, 6
2.8	Identify incident scenarios with their consequences	Not addressed	N/A
Phase 3 – Risk Estimation			
3.1	Assess threat likelihood of occurrence (probability)	Not addressed	N/A
3.2	Assess vulnerability	Not addressed	N/A
3.3	Assess existing controls implementation status	Not addressed	N/A
3.4	Assess business impact	Not addressed	N/A
3.5	Determine risk level	Not addressed	N/A
Phase 4 – Risk Evaluation and Treatment			
4.1	Decide on risk acceptance criteria	The standard addresses that an organisation should make decisions on whether to own, transfer, or treat strategic risk based on the application of its risk criteria for eDiscovery (ISO, 2018b).	ISO/IEC 27050-2: page 6
4.2	Prioritise risk	Not addressed	N/A
4.3	Recommend a risk treatment plan	Not addressed	N/A

2.7.3 Proposed Solution

Based on the literature review and the discussion in Section 2.7.2, the researcher concludes that the current ISO/IEC 27050 does not have well-defined security risk management elements that are suitable for the eDiscovery processes. Therefore, a set of considerations will be proposed in Chapter 3 to fill in the identified gaps and introduce a reference risk management framework model.

These considerations can be filled in by applying the following steps:

- Identifying the required artefacts (both existing and missing) of the proposed model such as context, target description, security objectives, assets, and legal aspects.
- Developing risk evaluation criteria, impact assessment method, examples of typical threats, examples of vulnerabilities and threats, threat assessment method, and technical vulnerability assessment method.
- Designing and developing a model flowchart diagram and process (input, activity, and output) taking into consideration asset valuation, risk identification, risk estimation, risk evaluation, and risk treatment.
- Identifying constraints for risk modification considering time, technical, operational, ease of use and other constraints.
- Aligning the proposed framework with the international best practices (e.g., ISO/IEC 27005).
- Integrating the proposed framework model with the ISO/IEC 27050 standard.

2.8 CONCLUSION

This chapter explores basic concepts that are essential for reviewing current risk management frameworks. More specifically, it identifies the current issues with the ISO/IEC 27050 standard and highlights the gaps. It also suggests a set of concerns that need to be considered to fill in the identified gaps.

The ultimate advantage of having a standardised risk management framework model is to have a common ground between different contexts in an eDiscovery domain. It is a complex task to set criteria or common properties for selecting a fit-for-purpose risk management methodology from a variety and range of frameworks due to the multiple mappings and context-driven lexicons. However, for the scope of this research

and based on the literature reviewed, five risk management frameworks have been chosen in the context of information security: ISO/IEC 31000 standard, ISO/IEC 27005 standard, NIST risk management, ENISA risk management, and the Risk IT framework.

Each risk management standard is reviewed in detail by explaining its document structure, main phases/processes, supporting security controls catalogue, and expected artefacts (deliverables/outcomes). A comparison between the selected risk management standards in terms of their risk method/phases and the supported security controls catalogue was completed. During the research investigation, it has been found that ISO/IEC 27050 does not provide a detailed description of how to perform risk analysis and manage the identified risks. Instead, it provides high-level requirements for the whole ESI investigation process. Although ISO/IEC 27050 uses ISO/IEC 30121 as the risk governance framework reference for a digital forensic process, the ISO/IEC 30121 does not provide a holistic approach for managing risk in the digital forensic context. Instead, its primary emphasis lies in preparing an organisation for digital investigations in advance of their actual occurrence. Moreover, the ISO/IEC 27050 does not cover all elements of a risk management framework as reported in this chapter.

Finally, this chapter provides the preliminary analysis for Chapter 3. Chapter 3 discusses the problem statement and methodology in response to the identified gaps. Moreover, Chapter 3 focuses on the methodologies employed to address identified gaps, research questions, hypotheses, and steps taken to objectively research while addressing the issues that have been discovered in this chapter. Chapter 3 will now define a methodology and methods for filling the identified gap.

Chapter 3: Methodology

3.0 INTRODUCTION

Figure 3.1 shows the summary of the thesis structure based on the proposed research methodology. The dashed lines show the roadmap for Chapter 3 which is Phase 3 (Artefact Design and Development).

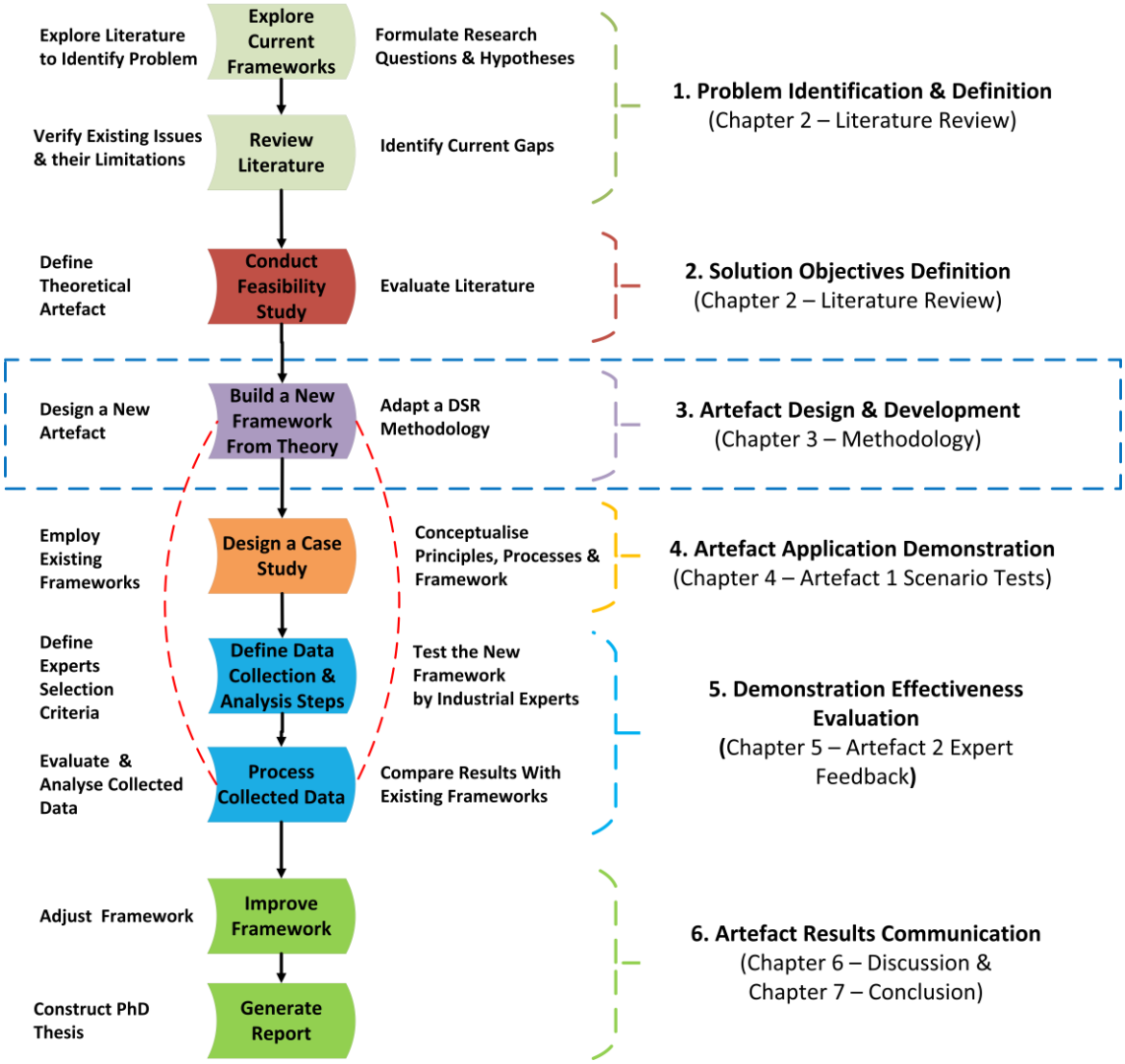


Figure 3.1: Chapter 3 Roadmap

The selection of a suitable and systematic research method is crucial for the successful completion of any research endeavour. A method encompasses the tools, procedures, or techniques used to execute a process in a coherent, structured, and systematic manner (Berndtsson et al., 2008).

Within the scope of this research, the term method denotes a systematic and structured approach to problem-solving, encompassing elements such as a hypothesis or

proposition formulation, adaptive research methodology design, theoretical framework description, data collection, hypothesis testing, results interpretation, and the formulation of conclusions subject to evaluation by independent domain experts. Chapter 3 introduces a conceptual model for security risk management and outlines the customised DSRM. This chapter is structured as follows. Section 3.1 defines the research design research concepts and their principles. It also describes three studies related to enterprise risk management frameworks with a brief comparison between them. Next, Section 3.2 focuses on addressing the identified primary research and its associated sub-questions, research hypotheses, and their mapping. Section 3.3 presents two well-known research methodologies in DS used in the IS field.

An adaptive/customised DSRM is defined in Section 3.4, along with its main six phases and associated steps: problem identification, solution definition, solution design, demonstration, evaluation, and communication. This section also identifies a set of research strategies, research methods, and data collection methods used in this research to obtain the research data requirements. Section 3.4 explains the supporting tools used to model and conduct the risk analysis including Monte Carlo simulation, FAIR-U risk calculator, and Archi model design. Moreover, specific data collection and analysis techniques are briefly discussed in alignment with the data requirements presented in Section 3.3. On the other hand, this section describes the FAIR model for risk estimation and its ontology, and the proposed integrated approach between the FAIR model and the proposed security risk management framework.

Section 3.5 introduces the proposed conceptual model with a high-level description of risk management building blocks (principles, framework, and processes). The section briefly describes the strawman approach used in this research to construct the first theory-based framework artefact. A set of modelling concepts with characteristics of each concept and their relationships in an actual organisational context are presented in this section. This is to help the researcher understand, manage, and express security risks in a visual relational format. A graphical presentation of the Artefact 1 security risk management framework is given in this section with a high-level description of its main phases. Section 3.6 then addresses two key limitations of the proposed research. This chapter ends with the main conclusion and connection to Chapter 4 in Section 3.7.

3.1 OTHER STUDIES

DSR is a qualitative process that encompasses the simultaneous generation of knowledge regarding the methodology employed to design artefacts and the actual design of those artefacts. On the other hand, DS is a powerful tool that helps researchers to answer questions relevant to human issues by designing representational artefacts. Those artefacts contribute to creating new knowledge in the body of scientific evidence, providing an initial understanding of problems that the researchers try to solve, and then establishing a conceptual model for the characteristics of research outputs. Hence, the goal of DS is to turn knowledge into value that people use (Hevner & Chatterjee, 2010). The essential principle of DSR entails acquiring knowledge and comprehension of a design problem and its corresponding solution through the iterative development of an artefact (Hevner & Chatterjee, 2010).

Two studies focused on evaluating the current Enterprise Risk Management (ERM) practices using a DSR method. Almeida et al. (2019) explained various approaches that allow organisations to adopt and adapt the ISO/IEC 31000 standard within their environment. On the other hand, in a study conducted by McShane (2018), the objective was to explore the evolution of the progression of ERM and suggest a DS approach to enhance the implementation of ERM implementation in organisations. The current ERM practices operate in a silo manner, limiting the sharing of risk information and the achievement of an organisation-wide view of risks (Almeida et al., 2019). Furthermore, the current ERM research does not provide common standards when dealing with a complex evolution due to fragmented disciplinary treatment (McShane, 2018). To close the identified gaps, Almeida et al. (2019) suggested that incorporating Enterprise Architecture (EA) models and tools can simplify the complexity inherent in the ISO/IEC 31000, thereby facilitating a better understanding of diverse stakeholders.

A third study was conducted by Mishra et al. (2019) aimed at exploring the factors affecting ERM and introducing a framework for identifying and describing the ERM artefacts. The current risk identification approach was found inadequate in addressing the growing complexity of risks and identifying potential exposure of organisational resources over time. The authors surveyed to prove that the proposed framework could be effectively employed for risk identification and management in any organisation.

Table 3.1 provides a brief comparison between the three studies above.

Table 3.1: A Comparison Between Three Studies in Developing ERM Using Various Research Methods

Author & Year	Research Question	Problem Identified	Research Method	Open Issue(s)	Future Work
Almeida et al. (2019)	How to use an EA tool to create a new ISO/IEC31000 metamodel, enabling a deeper comprehension of the value of assets?	ISO/IEC 31000 standard is excessively abstract and has a lot of ambiguous terms and definitions.	DSR	The lack of theoretical foundation and limited scientific studies on ISO/IEC 31000 standard. The absence of an official ArchiMate risk management extension leads to an accurate interpretation of mappings. The insufficient understanding and familiarity with the ArchiMate language and EA techniques.	Conducting more pilot demonstrations to summarise the long-term risk management performance of organisations. Delivering general risk management awareness to the organisations.
McShane (2018)	How to design a proscribed method to implement ERM within an organisation in an effective way and resolve the existing issues (e.g., change	Change management is continuous and long-term planning is a difficult aspect, especially when dealing with uncertainty in organisations.	Synthetisation practice using DS.	Various group of participants is required to successfully implement change management initiatives. Develop the necessary organisational change	Conducting more intensive efforts in the holistic ERM philosophy. Encouraging collaboration among diverse disciplines to

Author & Year	Research Question	Problem Identified	Research Method	Open Issue(s)	Future Work
	management initiatives and uncertainty)?			capabilities to support the implementation of an effective ERM approach that is tailored to the specific needs of the organisation, rather than relying on a one-size-fits-all.	advance research in the field of ERM.
Mishra et al. (2019)	What are the proactive approaches for assessing and managing enterprise risk exposure within organisations?	Risk identification is a fragmented area. It is difficult to identify risks if there is no clear linkage between individual organisational resources and risk.	Online survey	Decision-making based on human judgment does not always rely on data-driven approaches. The proposed framework is not formally tested.	Taking into account the second-order interactions within the risk classes.

3.2 RESEARCH QUESTIONS AND HYPOTHESES

Research questions and hypotheses play a critical role in any research. A research question is a knowledge query that the research aims to answer, considering certain factors. It helps determine the design requirements for an artefact to address the identified research gap. Essentially, the research question is formulated based on the research problems, aiming to solve them and achieve the research objectives. On the other hand, the hypothesis is a statement of expectation that will be evaluated and tested by the research.

Based on the literature review presented in Chapter 2 and the problem identification described in Section 3.4.1.1, a primary research question and three sub-questions have been formulated and stated with the three hypotheses to support those questions.

3.2.1 Research Questions

Figure 3.2 illustrates the process with five stages of how the primary research questions and their associated sub-questions have been identified.

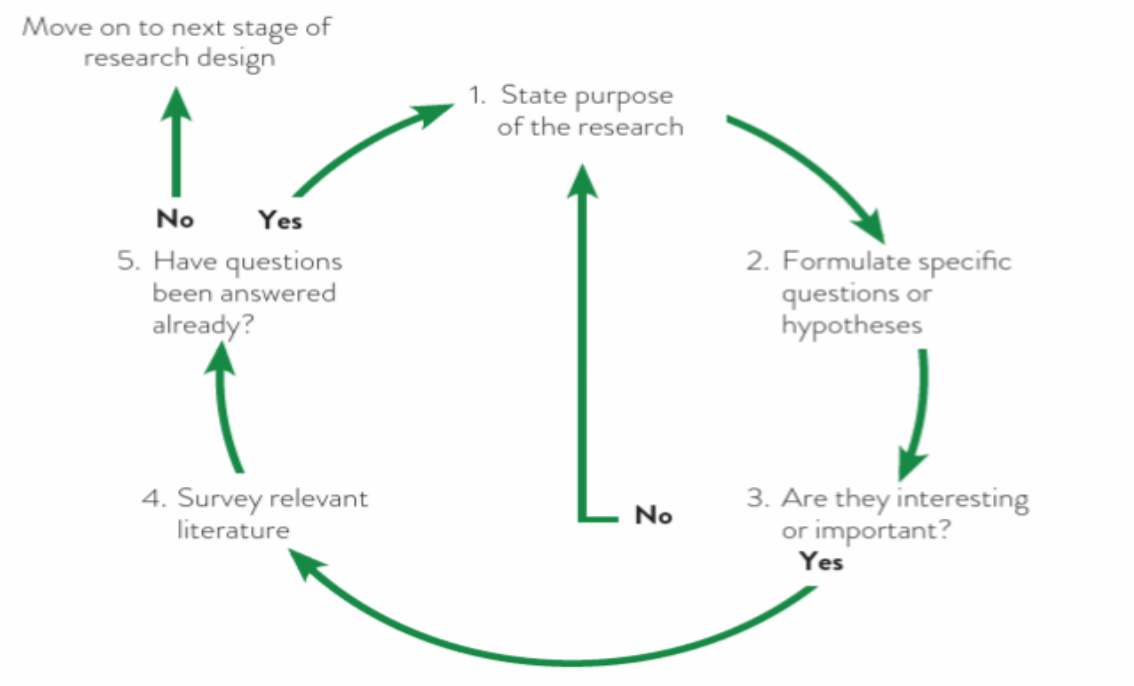


Figure 3.2: Research Questions Identification Process (Collis & Hussey, 2021, p. 94)

At each stage in the process, the researcher reflected on relevancy and discussed it with the research supervisors. The researcher searched the relevant literature to see if the identified research question has been answered. The outcome of that investigation indicated that this research could produce new findings in the security risk management

area. Consequently, it would make a valuable contribution to the existing body of knowledge as outlined in Chapter 6.

Based on the above discussions, the primary research question is formulated as: "**What framework aligns the current ISO/IEC 27050 standard with the ISO security risk evaluation framework in a cost-effective way**?". The sub-questions to clarify the primary research question are:

- **SQ1**: What are the main limitations and weaknesses of the current ISO/IEC 27050 standard in the context of risk management processes?
- **SQ2**: What design components improve the risk identification capabilities of the current ISO/IEC 27050 standard?
- **SQ3**: What steps are necessary to integrate the new artefact with the current ISO/IEC 27050 standard?

3.2.2 Research Hypotheses

Three research hypotheses have been designed to support answering the previous research sub-questions. The three research hypotheses are:

- **H_1**: The proposed framework model adds value with a shift from requirements approach to a referenced standards approach.
- **H_2**: The new artefact better identifies the risks associated with eDiscovery.
- **H_3**: The new artefact is a cost-effective risk identification method for organisations.

Figure 3.3 presents the relationships between the primary research questions, three sub-questions, and the three hypotheses.

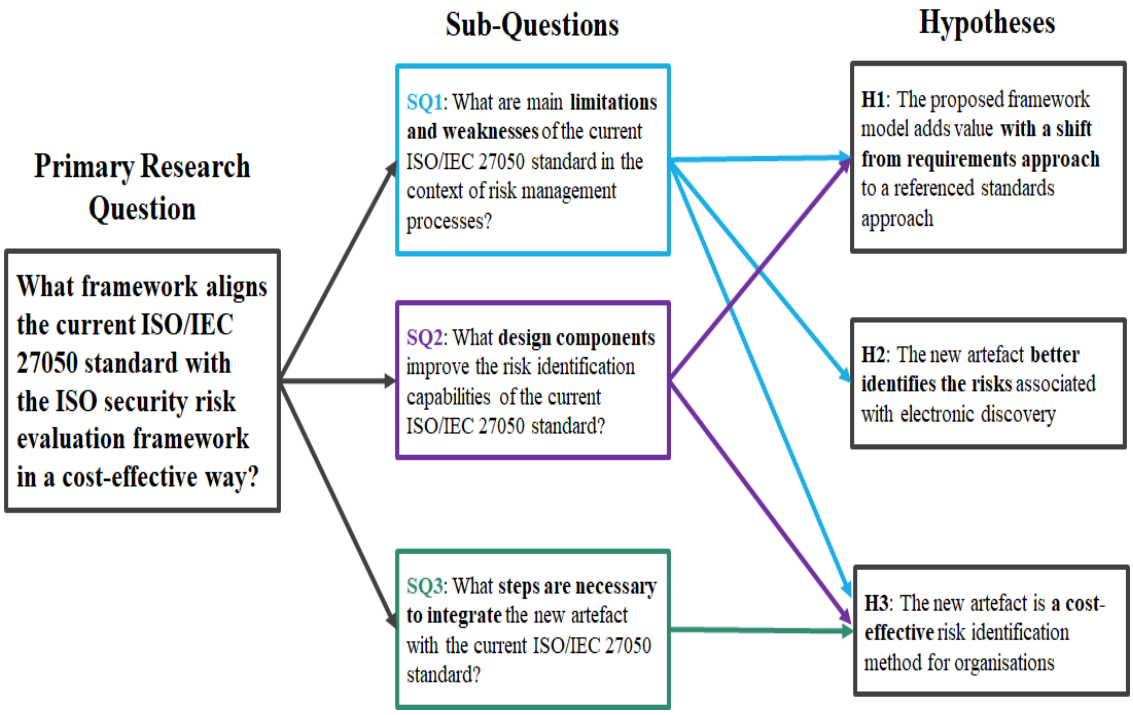


Figure 3.3: Research Question, Sub-Questions, and Hypotheses Relationships

3.3 RESEARCH DESIGN IN INFORMATION SYSTEM

A methodology can be described as a set of principles, practices, and procedures employed in a specific field of knowledge. Within this context of DSR, there are three primary attributes. Firstly, conceptual principles are established to define the essence of DSR and its objectives. Secondly, practice rules are established to provide guidance. Thirdly, procedures are established for conducting and presenting the research (Peffers et al., 2007). However, DSRM goes a step further by providing a formal process model for conducting DS and developing relevant artefacts. Furthermore, DSRM serves not only to create artefacts but also to address research questions. Depending on the research's goals and characteristics, a researcher can tailor the processes to achieve either innovative or confirmatory outcomes (Johannesson & Perjons, 2014).

The following subsections describe two well-known methodologies used in the IS disciplines for more than a decade.

3.3.1 Design Science Research Methodology

The DSRM is chosen to guide this research project (Wieringa, 2014). It is chosen because the researcher needs to take a theoretical construct from the literature review and improve it. DS focuses on designing and investigating artefacts that are intended to interact with a problem context, aiming to improve that context (Wieringa, 2014). DSRM is a framework

for guided action to deliver an artefact of value. The value is for both theory and practice as shown in Figure 3.4.

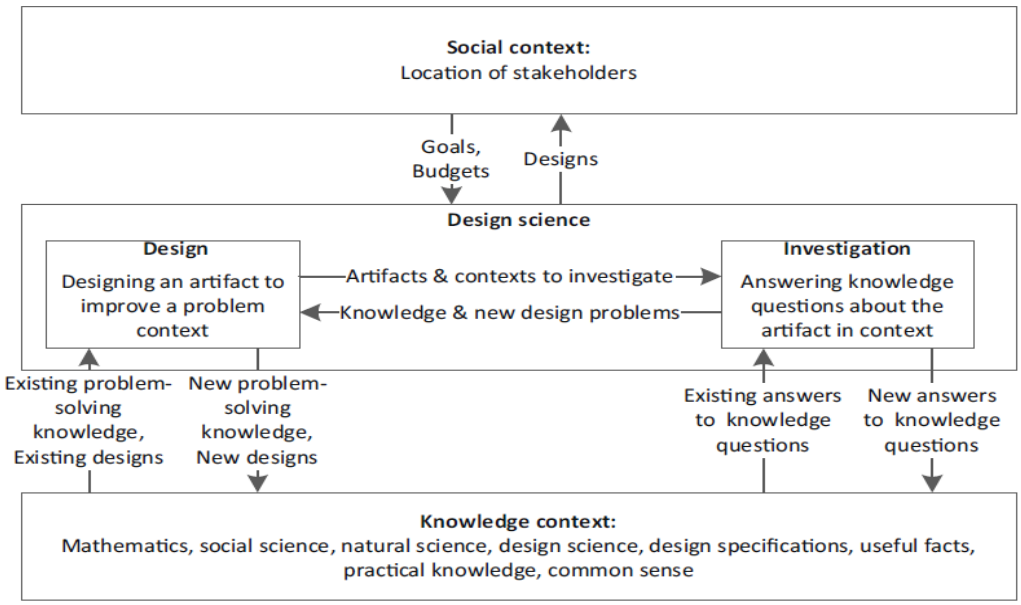


Figure 3.4: A Framework for Design Science (Wieringa, 2014, p. 7)

In addition to a conceptual framework, DSRM provides a lifecycle of actions that contribute to the development of an artefact until its utility. In Peffers et al. (2007) model, a researcher has four potential entry points and the options to initiate the design of an artefact. The model has the potential to deliver design types at each of the first four phases and evaluation criteria for effectiveness and efficiency in different contexts. There is a forward propagation towards the market and feedback loops for improvement as depicted in Figure 3.5.

The final phase of the DS research methodology is referred to as communication. This phase is specifically designed to enable the researchers to utilise various scholarly electronic databases to convey the outcome of their study. This communication aspect involves sharing information about the problem's significance, the design artefact, the robustness of its design, and its effectiveness with other researchers and practitioners in the field (Dresch et al., 2014). Additionally, it recommended that researchers conclude their studies by discussing the implications of their research findings for practical applications. March and Storey (2008) emphasise the importance of contributing to the advancement of general knowledge while simultaneously enhancing the practical state of affairs in the field when conducting DS research.

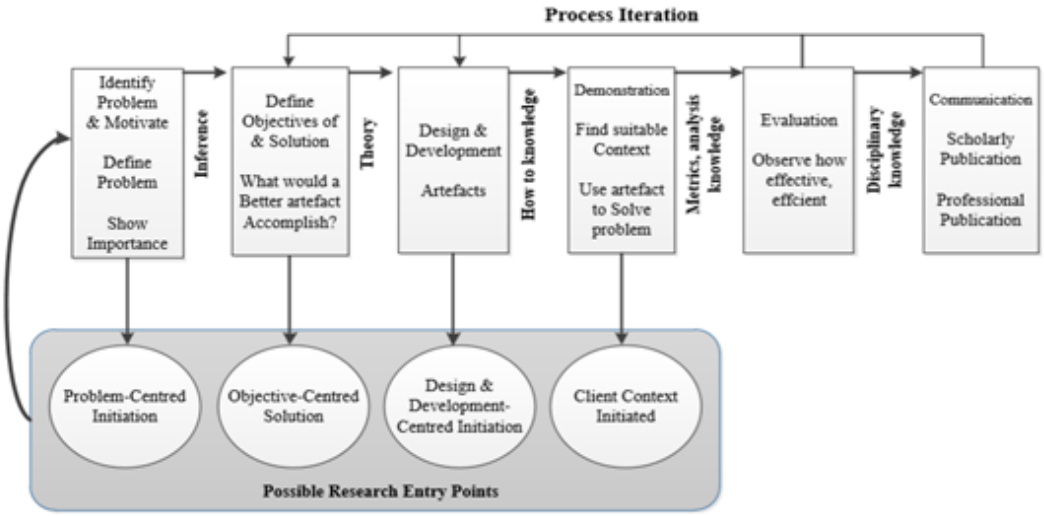


Figure 3.5: DS Research Methodology (Peffers et al., 2007, p. 54)

However, the Peffers' model does not specify methods on how to perform any step in the lifecycles, but rather only tells what to do when a decision is made. Hevner et al. (2004) provided some criteria to assess the originality of artefacts within the field. These criteria involve evaluating the models and methods created in the context of DS based on completeness, simplicity, coherence, user-friendliness, and the quality of outcomes produced by the method. Additionally, rigorous testing and feedback are required for a researcher to claim the novelty, usefulness, or relevance of an artefact as illustrated in Figure 3.6.

The gaps in DSRM have been filled by other researchers as well. Wieringa (2014) offers a wide range of methods for testing and improving an artefact. What is applied and how it is used is dependent on the artefact's context, purpose, and use. Relevant to this research and scenario tests are specified in detail, and expert feedback is offered as another way to move a theoretical artefact into use.

In this research, the theoretical artefact (i.e., strawman framework Design 1) developed from phases 1, 2, and 3 in the Peffers' model are taken, and then Phase 4, where "How to knowledge" is used to test the relevance of the framework. To achieve this, three scenarios were taken from the literature (see Sections 4.1, 4.2, and 4.3 in Chapter 4) and the framework was applied to mitigate risks in the eDiscovery processes. The feedback from the testing is used to improve the framework and create a Design 2 version.

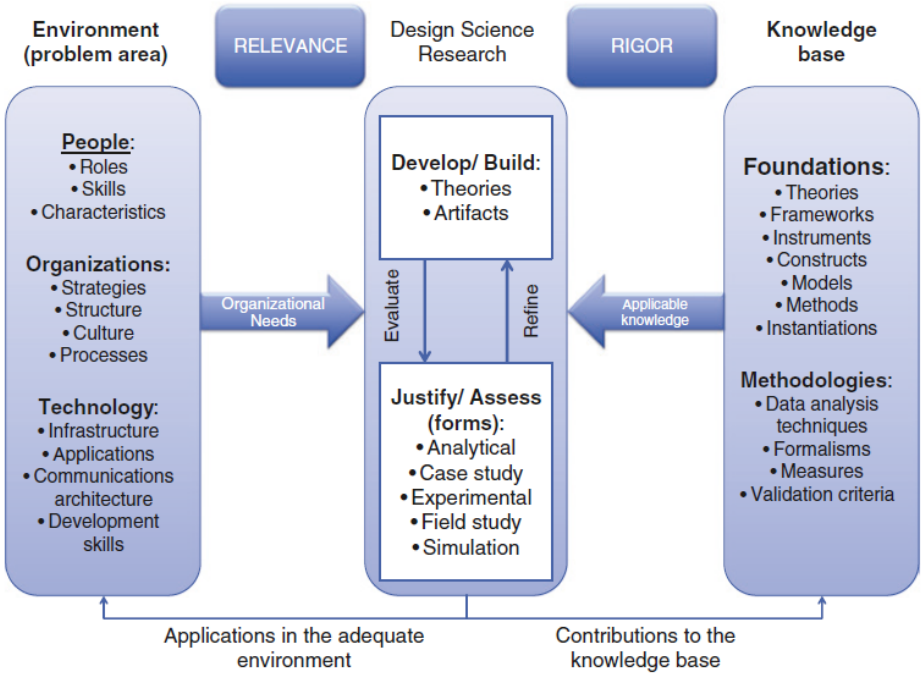


Figure 3.6: Relevance and Rigor in DS Research Adapted from Hevner et al. (2004), Source: (Dresch et al., 2014, p. 69)

The Design 2 version is then taken to industry experts for feedback under the AUTEC dispensation for Expert Feedback 6.1 using the standard feedback sheet derived from Hevner et al. (2004) and criteria for artefact rigour and relevance. The experts are selected from the ISACA Auckland database for their participation in eDiscovery work and security audit processes. The feedback from the industry is then used to create a Design 3 prototype version of the framework.

3.3.2 Design Science Research Process

A research process provides a systematic method that enables researchers to uncover solutions or answers to questions and problems using scientific methods. It supports researchers to create an artefact that consists of four main components (Offermann et al., 2009):

- Constructs: terminology and symbols
- Models: abstraction and representations
- Methods: algorithms and approaches
- Instantiations: implemented and prototype systems

Offermann et al. (2009) propose a Design Science Research Process (DSRP) that integrates both qualitative and quantitative research methods. This process can be used to conduct DS in IS research. In general, the DSRP comprises three main phases and each phase has a few steps as listed in Figure 3.7.

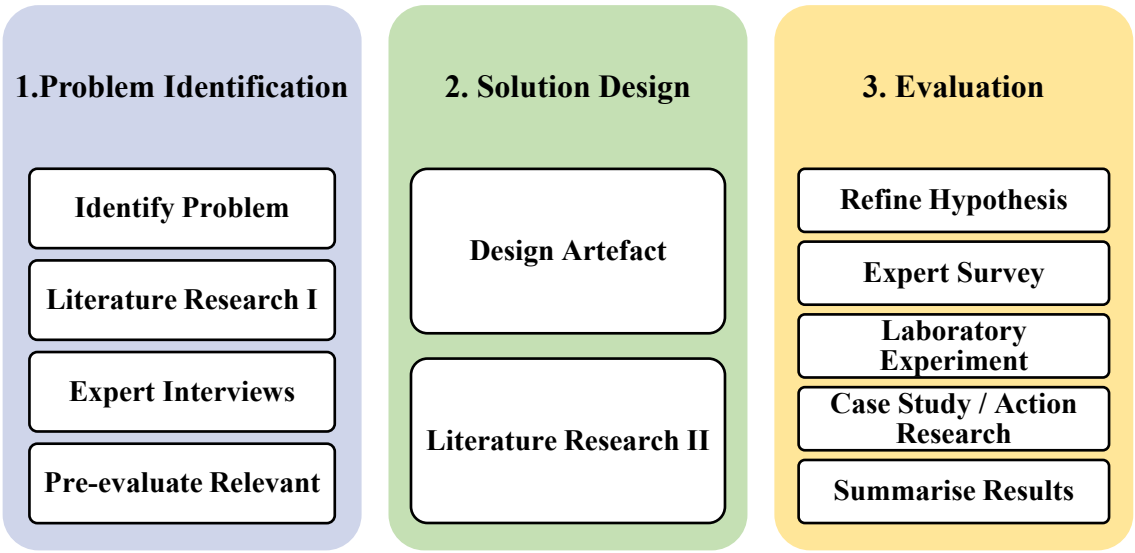


Figure 3.7: The Design Science Research Process Phases and their Steps (Offermann et al., 2009)

Figure 3.8 illustrates the process flow of the DSRP, where the arrows represent transitions between steps, and dotted lines represent less commonly used transitions. It is important to note here that the steps are not always carried out sequentially; they often reference each other. The DSRP method aligns with the DSRM presented by Peffers et al. (2007) except for the publications activity. The authors of the DSRP pointed out that the publications do not include a process themselves. It important to note that "Pre-evaluation relevance" step shown in both Figure 3.7 and Figure 3.8 involves creating and refining a research hypothesis that connects a proposed solution to a problem's potential effects, while gathering practitioners' input to assess its relevance and identify plausible pre-assumptions (Offermann et al., 2009).

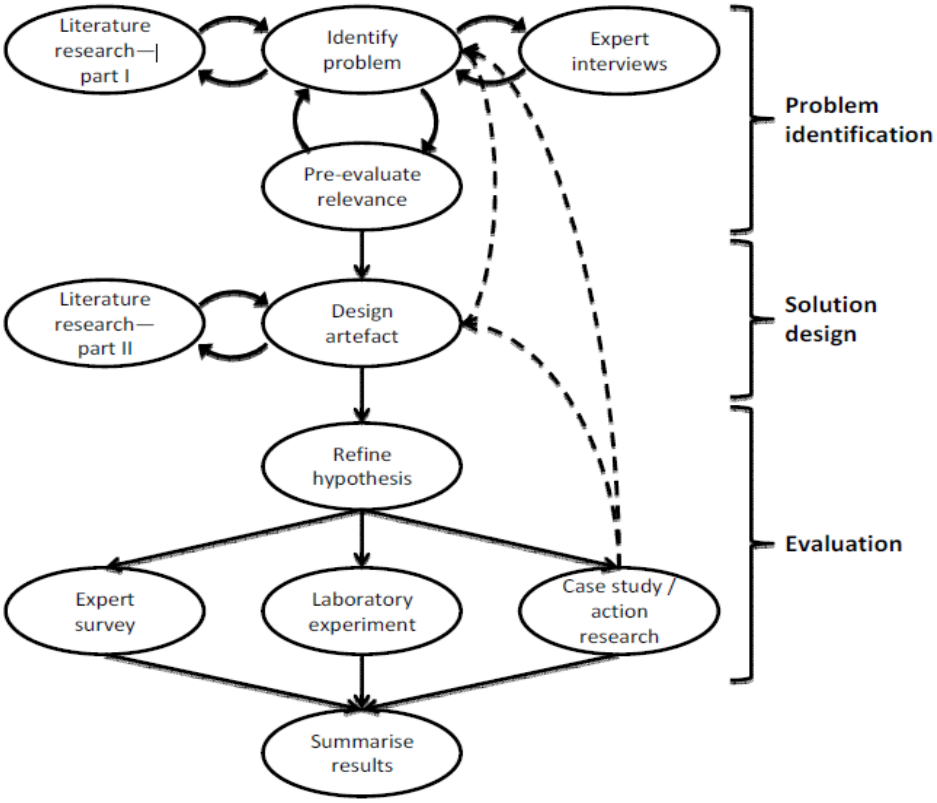


Figure 3.8: Design Science Research Process Method (Offermann et al., 2009, p. 5)

3.4 APPLYING ADAPTIVE DESIGN SCIENCE RESEARCH METHODOLOGY

This research involves conducting a DS investigation, which serves as an exploratory study aimed at creating, reviewing, evaluating, and potentially redesigning a specific artefact. The proposed artefact is subsequently assessed through a data collection method. The defined hypotheses are then tested using qualitative analysis employing a quasi-judicial method, which involves utilising a rational argument to interpret the data (Collis & Hussey, 2021).

Based on the previous discussion, the researcher used an adaptive research process based on the combinations of both the DSRM and DSRP, with minor adjustments. This ADSRM approach provides a process to define the problem statement, design risk management framework artefacts; and ultimately produce a new solution.

3.4.1 Using Adaptive Design Science Research Methodology

Figure 3.9 presents an overview of the ADSRM approach phases and their associated steps. There are six phases with various steps split into three main parts: Inputs (Phases 1

and 2), Processes (Phases 3, 4, and 5), and Outputs (Phase 6). The arrows represent a transition from one step to the next. These phases are as follows:

- **Identify Problem and Motive** – Articulate and emphasise the significance of the problem.
- **Define Objectives of a Solution** – Determine the desired characteristics and qualities of an improved artefact to address the problem.
- **Design and Development** – Construct and develop an artefact of the proposed framework.
- **Demonstration** – Apply the proposed framework artefact in a suitable context to solve the problem.
- **Evaluation** – Assess the effectiveness and efficiency of the proposed framework, and then iterate on the design if necessary.
- **Communication** – Publish scholarly works to disseminate findings and insights. The following subsections provide a high-level description of the application of the ADSRM approach to the risk identification problem of the ISO/IEC 2050 standard.

3.4.1.1 Phase 1 – Problem Identification and Definition

The first phase of the ADSRM approach identifies the particular research issue under investigation and provides a rationale for the importance of the proposed solution. The main activity of this phase is to explore current frameworks and conduct a literature review, and then formulate research questions and hypotheses.

To define a problem, extensive literature research was conducted to review what risk management frameworks existed as discussed in Chapter 2. Figure 2.5 in Chapter 2 presented the research approach used to study and analyse the current risk management frameworks. A gap analysis for the ISO/IEC 27050 standard was carried out. This analysis showed that the current ISO/IEC 27050 standard does not provide a detailed description of how to perform risk analysis and manage the identified risks. Instead, it provides high-level requirements for the whole ESI investigation process. In addition to that, the ISO/IEC 27050 standard does not cover all elements of a risk management framework as compared to other well-known frameworks and best practices.

During this phase, the general research hypothesis is formed. Although the hypothesis has been identified, it is continuously adjusted as the research process evolves, and hence it is fed into the problem specification iteration.

3.4.1.2 Phase 2 – Solution Objectives Definition

The second phase of the ADSRM approach defines the objectives of a desirable solution and shows how the proposed solution is better than the current solutions. The core activity of this phase is to conduct a feasibility study to understand what is possible and what is feasible for this research. This helps in determining the research's motivation for the current solution. It is worth noting that the literature review carried out during this phase differs from the literature review performed during the problem identification phase. The first literature review focuses on the current methods whereas the second one centres on the evaluation and comparison of current risk frameworks.

3.4.1.3 Phase 3 – Artefact Design and Development

The third phase of the ADSRM approach designs a solution based on the results of the problem identification phase and the established solution objectives. The main activity of this phase is to create and adapt the DSRM, and then design a conceptual model.

Before starting to design a new security risk management framework, existing frameworks were studied, analysed, and compared. The purpose of that was to assess the strengths and weaknesses of the current methods. The outcome of the comparison between the candidate methods has initially led to the decision of adapting and adjusting a combination of ISO/IEC 31000 and ISO/IEC 27001 frameworks analysed in the literature review.

3.4.1.4 Phase 4 – Artefact Application Demonstration

The fourth phase of the ADSRM approach provides initial proof of the proposed design by designing and selecting testing scenarios (i.e., ESI use cases). The selected testing scenarios are used as an evaluation method to refine the defined hypothesis. This refinement aims to define a more precise scope by dividing the general hypothesis into smaller hypotheses, thereby facilitating the evaluation process. In this research, a group of experts are chosen to evaluate the applicability of the proposed framework, its usability, and its efficiency. The structure of the proposed model consists of three building blocks: principles, framework style, and processes and their relationship as described in Section 3.5.2.1, 3.5.2.2, and 3.5.2.3 respectively.

3.4.1.5 Phase 5 – Demonstration Effectiveness Evaluation

The fifth phase of the ADSRM approach involves evaluation the proposed artefact or the problem statement and making the required adjustments based on the evaluation

outcomes. This phase aims to iterate back to the initial state and refine the artefact or problem statement as needed.

The focus of this phase is to collect data and then evaluate and analyse the collected data. Qualitative analysis is employed in this research that focuses on analysing the expert feedback. The industrial expert's evaluation is the key input to improve the proposed artefact.

In this phase, data analysis is conducted using a quasi-judicial method, which involves a rational argument to interpret qualitative data. The quasi-judicial technique is an adequate method to interpret practical data. Unlike delaying data analysis until the end of the study, this method ensures that qualitative analysis is promptly interpreted. By establishing standard procedures and protocols for interpreting data, the authenticity of the results is assured (Collis & Hussey, 2021).

During this phase, it is important to compare the results between the existing frameworks and the proposed framework, so that any improvement is justified.

3.4.1.6 Phase 6 – Artefact Results Communication

The sixth phase of the ADSRM approach communicates the research outcomes to researchers and the relevant audience. This phase produces the outcome of the research. After the evaluation phase, adjustments are implemented to enhance the proposed framework as part of the improvement process. Ultimately, the primary findings of the research are disseminated through a PhD thesis, encompassing elements such as the problem definition, literature review, hypothesis development, data requirements and analysis, results, discussion, and conclusion. Furthermore, the intermediate data can be published in the form of a Journal articles and Conference papers.

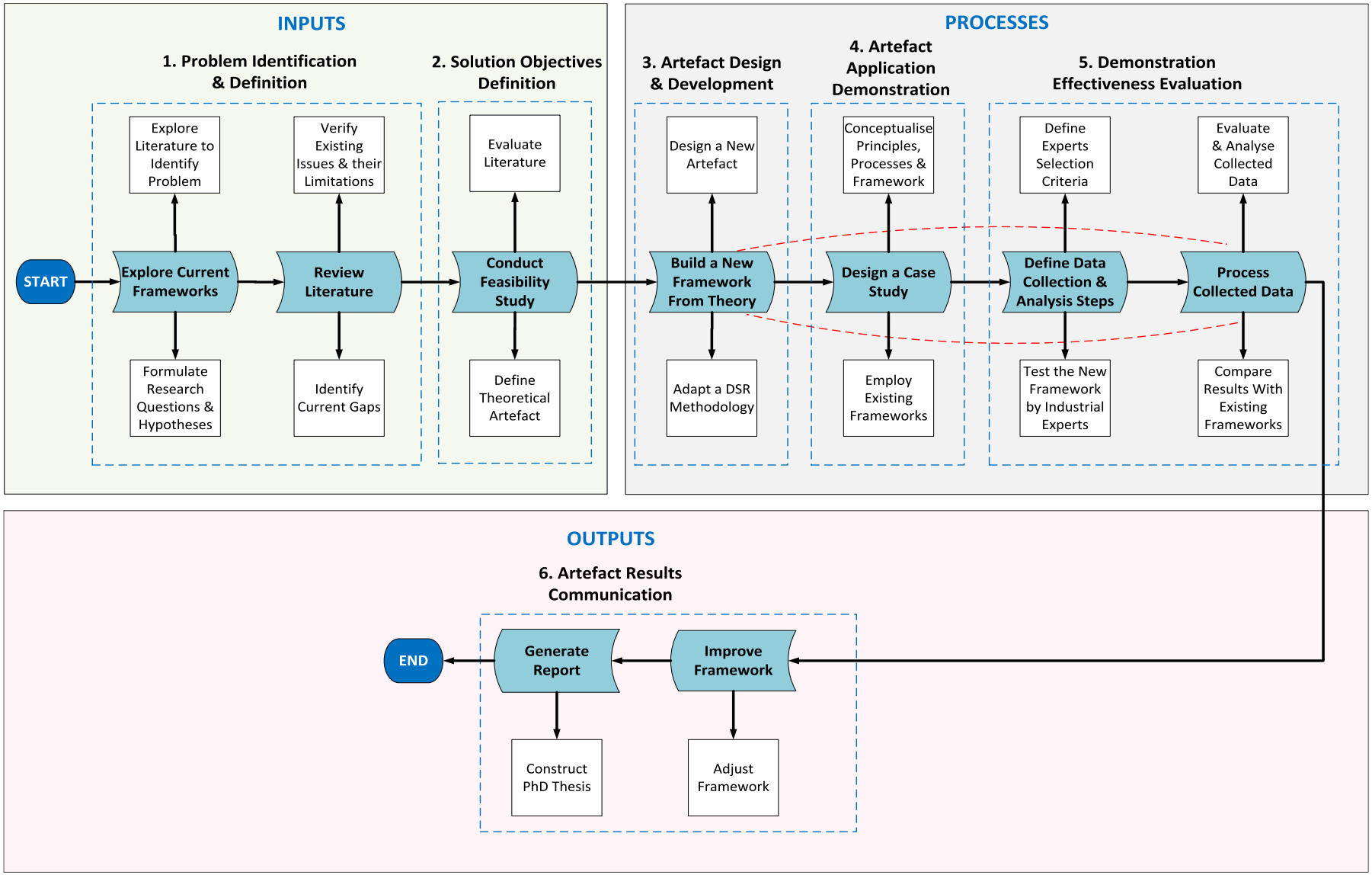


Figure 3.9: Researcher's Adaptive Design Science Research Method with Process Level Design and Deliverable Elements

3.4.2 Data Collection Structures

Data requirements are derived from research strategies and research methods. Research strategies are used to support researchers in identifying a practical problem, designing requirements, and evaluating artefacts. On the other hand, research methods are used to help researchers in defining how to gather and analyse data such as using a questions template, requesting feedback, or performing content analysis. Consequently, a research strategy provides a broad approach, targeting a specific audience, while a research method offers a useful technique or tool to carry out a specific task (Johannesson & Perjons, 2014).

3.4.2.1 Data Collection and Analysis Methods

Analysing data helps transform a large amount of data into meaningful pieces of information (Johannesson & Perjons, 2014). Data analysis methods can be categorised into either qualitative or quantitative approaches. However, it is important to point out that the combination of qualitative and quantitative methods is achievable when adopting DSR methods in the IS disciplines (Hevner & Chatterjee, 2010).

Selecting a research strategy relies on the objectives and attributes of the specific research being conducted. However, Johannesson and Perjons (2014) define three main aspects that should be considered when selecting a research strategy. The strategy should:

- Enable the researcher to seek answers to the research question at hand.
- Facilitate access to various data sources (e.g., people, documents, laboratory equipment, computer software) based on the research needs.
- Ensure that the data is collected ethically (e.g., no harm, anonymous of participants, use data for research purposes only, keep data secured and confidential).

Johannesson and Perjons (2014) and Peffers et al. (2012) identified various methods for evaluating DSR. Table 3.2 provides a summary of several practical research strategies.

Table 3.2: Research Strategies (Johannesson & Perjons, 2014; Peffers et al., 2012)

No.	Research Strategy	Purpose
1	Experiment	Explore cause and effect relationships by conducting a performance evaluation.

2	Survey	Examine specific aspects of a phenomenon to gain a comprehensive understanding.
3	Case Study	Delve deeply into a phenomenon with a clearly defined scope.
4	Grounded Theory	Create concepts and theories through the analysis of empirical data.
5	Action Research	Generate valuable knowledge by addressing practical issues and evaluating their effect on a real-world scenario.

In the context of this research, the researcher has selected a case study through testing scenarios as the main research strategy to support presenting the research results. The case study strategy provides several benefits over the other strategies. For instance, it provides as much information as possible about the problem that needs to be investigated. Additionally, it ensures that the research is investigated holistically, taking into consideration all relevant aspects of the real-world situation. Furthermore, case studies employ an artefact in a real-world scenario to assess the functionality and impact of an artefact within its environment (Johannesson & Perjons, 2014; Peffers et al., 2012). Case studies serve various purposes, such as creating research questions or hypotheses that can be applied in other studies.

Collecting data is a key task in any practical research study. There are numerous methods to collect data listed in Table 3.3 (Johannesson & Perjons, 2014).

Table 3.3: Data Collection Methods

Method	**Description**
Questions	A written document contains a set of constructive questions aimed at obtaining direct information, facts, and opinions from participants.
Interview	An interactive session between a researcher and a participant, where the researcher asks the participant questions to collect intricate and sensitive information.
Focus Group	A group interview format involves participants engaging in a discussion focused on a specific topic to gain insights from diverse perspectives.
Observation	The direct observation of phenomena by a researcher.
Documents	Utilising documents as a primary source of the data.

3.4.2.2 Data Collection Strategies

Qualitative data collection is an iterative process that aims to find a theme within the collected data. In this research, qualitative data analysis is used that focuses on three key approaches: thematic analysis, category coding, qualitative content analysis, and discourse analysis. This qualitative analysis focuses on analysing and describing data sources in a text format. Data is collected from the scenario tests and expert feedback. The first set of data is used to enhance the Strawman D1 framework, resulting in the improved D2 framework. The D2 framework is then shared with experts for their comments, and the data collected is utilised to develop the D3 framework.

Figure 3.10 illustrates the relationship between research strategies, data collection methods and data analysis approaches that were discussed in the previous subsections. As explained, the researcher chose testing scenarios as one of the research strategies. For collecting information from the experts, the researcher has selected the expert feedback method to analyse and evaluate the gathered data using a qualitative approach.

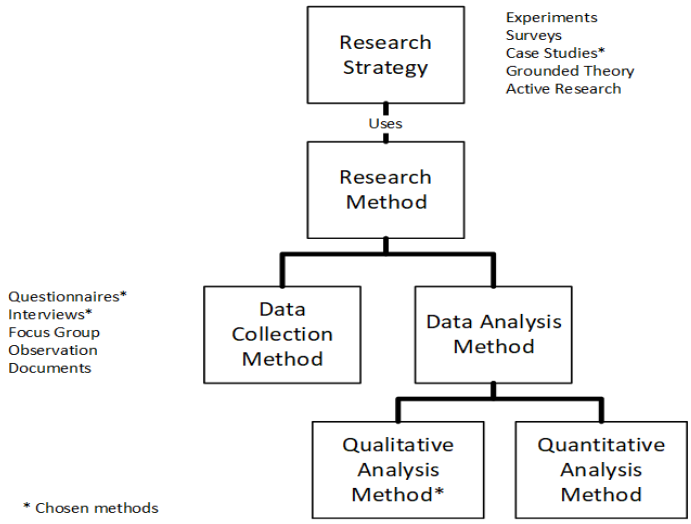


Figure 3.10: Research Strategies, Data Collection Method Data Analysis Approaches Relationship

In this research, a mixed methods approach has been selected (related to a triangulation principle) in which a research strategy (i.e., testing scenarios) and a data collection method are combined (i.e., a feedback template) to improve the accuracy of results and to expand the overall scope of this study. The main goal of this approach is to look at the identified research problem from a different perspective.

3.4.2.3 Expert Feedback

Expert feedback is collected using a feedback template specifically designed to gather reliable feedback from a selected group of people. The objective is to gauge their thoughts and emotions regarding the presented artefact, which would aid the researcher in addressing the formulated research question (Collis & Hussey, 2021). During this research, the template is shared with the selected experts to gather a significant amount of quantitative information. Additionally, as needed further qualitative information is gathered to complement the data collected.

In a researcher's approach, expert feedback is collected by gathering opinions from a selected group of experts. These experts neither convene nor are aware of the identities of other group members.

In qualitative research in the IS field, the ideal number of experts to involve is not a fixed or specific number (Guest et al., 2006). Rather, it can vary based on various factors, such as the research's nature, the research question, the research design, the level of data saturation, available resources, and data variability The researchers should focus on achieving data saturation, the point at which new experts no longer provide significantly new insights. This approach can influence sample size decisions (Guest et al., 2006; Marshall et al., 2013). Marshall et al. (2013) presents two crucial factors for determining the right sample size: grounded theory qualitative studies typically involve 20-30 experts, while single case studies usually encompass 15 to 30 experts.

Hevner and Chatterjee (2010) emphasise the importance of selecting group size carefully. While it may seem simpler and more cost-effective to conduct fewer, larger focus groups can reduce the effective sample size as there are fewer groups to compare. Furthermore, smaller and larger groups have distinct dynamic; smaller groups require greater participation from each member, whereas larger groups can lead to "social loafing". A lower boundary of 4 participants and an upper boundary of 12 participants are suggested. Depending on the approach taken to demonstrate the artefact to the group, large focus groups (more than 6) could be tricky in design research since the subject matter is more complex than traditional focus group topics, (e.g., a marketing campaign).

Based on the literature and the discussion above, this research involves the selection of ten experts for the feedback of the proposed framework model. Conducting expert evaluations can be time-consuming and resource intensive. Gathering feedback from ten experts strikes a balance between obtaining valuable insights and managing the cost and effort required for the evaluation process. A group of ten experts often provides

a diverse set of perspectives and opinions. These experts may have different backgrounds, expertise, and experiences, allowing for a broader range of issues to be identified. In many cases, it may be difficult to find and engage a larger number of experts who are willing and available to participate in the evaluation. Furthermore, a group of ten experts is more manageable and feasible. Processing and integrating feedback from a large number of experts can be challenging. With ten experts, it is easier to manage and make sense of the feedback and prioritise necessary improvements.

Figure 3.11 summarises the main steps involved in designing an expert feedback process.

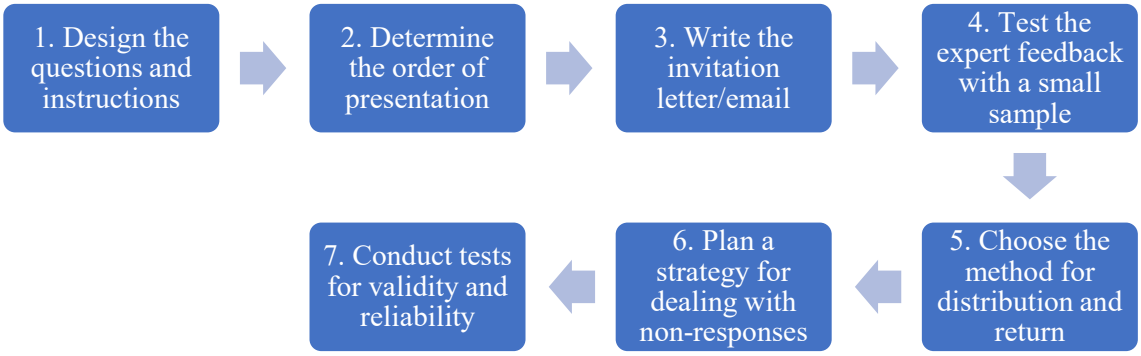


Figure 3.11: Designing Expert Feedback Process (Collis & Hussey, 2021, p. 191)

When communicating the feedback template with the selected group experts, the purpose of the research is explained because the respondents need to know the context in which the questions are being posed (i.e., briefly explaining the purpose of the research). This is achieved by attaching a cover letter to the feedback template.

A combination of closed and open questions is used to collect the experts' opinions. The closed questions are designed to collect objective opinions, and the open questions are designed to allow the respondents to communicate descriptively in their own words.

3.4.2.4 NVivo Analysis Tool

NVivo tool is designed to establish common qualitative techniques regardless of the research method used. NVivo is used in various fields such as coding, theory development, and data analysis, to aid in understanding research problems. In this study, NVivo was chosen as the appropriate qualitative analysis tool to answer research questions as well as enable the researcher to manage a substantial volume of data collected, enabling the creation of themes. NVivo manages, explores, and discovers

patterns in the data collected and increases the evidential support for the research results. However, it is important to note that NVivo cannot replace analytical expertise.

NVivo offers several benefits to this research. Primarily, it provides more flexibility on how data would be categorised in separate ways and improves the outcomes. Secondly, it minimises the time and effort to perform data analysis manually. Thirdly, it helps identify themes among the collected data and then draw evidential conclusions. Fourthly, it can analyse, classify, and categorise the data collected from experts and prioritise their feedback. Lastly, it can generate graphs and models to present the research results in an accessible way (Alam, 2021).

3.4.2.5 Data Collection and Analysis Process Steps

The main source materials of this research consist of structured data (e.g., a feedback template). In the context of the NVivo tool, the researcher sets up a case node for each interview for an expert participating in this research, then code to their nodes and case nodes. Then, the researcher explores the data collected with simple queries or charts; and uses memos to record the discoveries as illustrated in Figure 3.12.

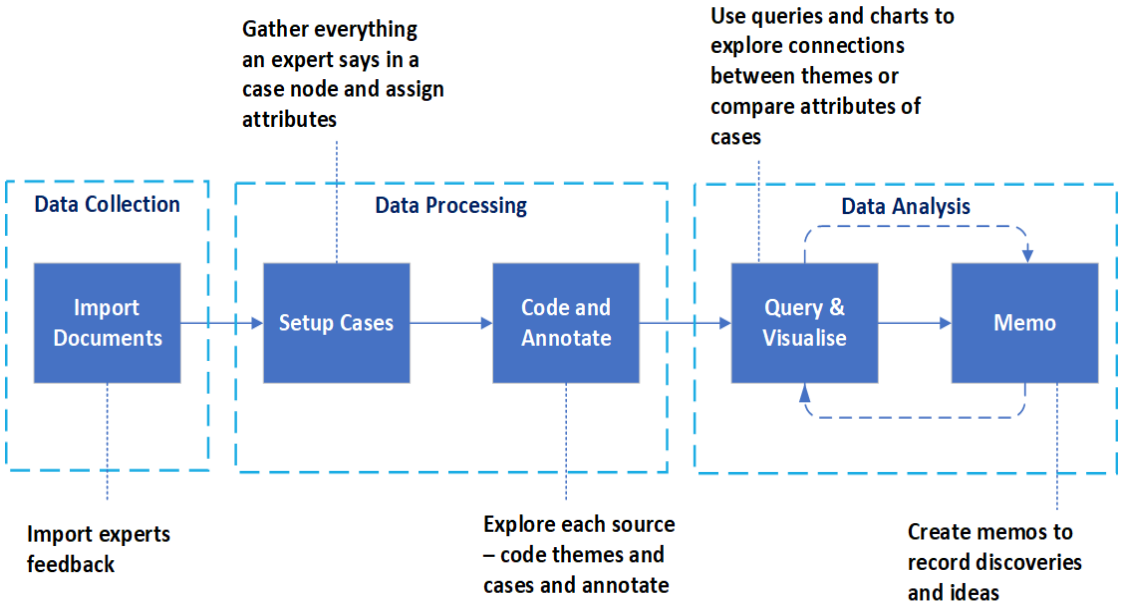


Figure 3.12: Data Collection and Analysis Process Adapted from NVivo Approach

Figure 3.13 illustrates the steps involved in the data collection and analysis process used in the research which is adapted from (Alam, 2021; Rashid et al., 2019). In general, there are three main stages of this process (Alam, 2021):

- Data familiarisation.
- Primary code creation, themes categorisation, code capturing, themes

revision and group formation.

- Pattern formation and establishing connections between themes, prioritising the creation of main categories.

To collect the required data, the first step is to define a set of criteria on how to select experts for feedback. The selection of participants in the research is based on their anticipated level of knowledge and the relevance of the information they possess about the research questions. Then, a list of experts (candidates) is created to start the initial contact. The next step is to give the willing experts a copy of the proposed framework, an introduction letter, and a set of questions (a feedback template) to respond to.

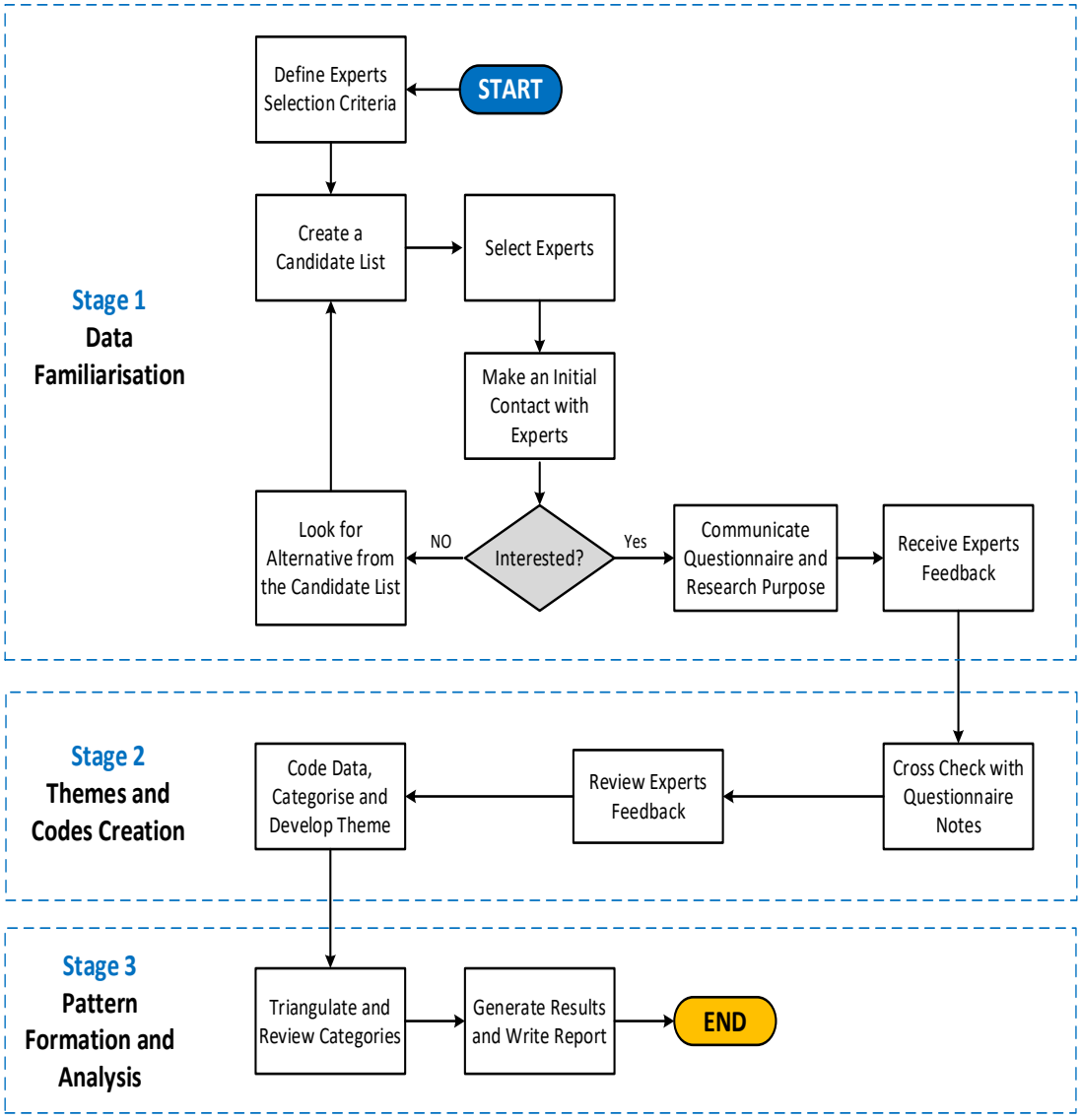


Figure 3.13: Data Collection and Analysis Process Steps

The data collected are imported to NVivo. Then, these data are clustered into codes, which can be based on frequent words, cases, or a combination of factors, to provide evidence for the research questions. From these codes, the themes are developed,

which comprise multiple codes and are associated with supporting texts. The query function is employed to gather insights regarding attitudes based on demographic attributes or to investigate the relationships and connections between them. Sub-categories are then grouped to create a linked memo and analyse the data. The last step of this process is to generate and summarise results, and then produce a final report.

In this research, a conceptual analysis method is used to analyse and interpret data collected from expert feedback. Thematic is selected as an analysis process to identify, analyse, and report themes from collected data.

3.4.3 Risk Modelling Tools

In this research, Monte Carlo Simulation and the FAIR-U tool are used to estimate the risk. Moreover, the Archi tool is used to create an ArchiMate 3.1 metamodel and sketch for the proposed artefact. The subsections below provide more details about the tools above.

3.4.3.1 Monte Carlo Simulation Tool

The Monte Carlo simulation is a robust modelling tool employed in the analysis of involved complex systems, as it enables a closer representation of reality. It utilises random numbers to estimate solutions to mathematical problems (Matsuoka, 2013). In other words, Monte Carlo is a useful tool for simulating sets of results by substituting a variety of values from a probability distribution for factors that possess inherent uncertainty. It repeatedly calculates results using a different set of random values from the probability functions (RiskLens, 2020). The definition of both Primary and Secondary Loss are exhibited in Sections 3.4.4.1 and 3.4.5.

In the context of risk analysis, Monte Carlo plays an important role in supporting risk analysts determine various aspects related to a specific loss event scenario. This includes estimating the number of primary loss events that occur, along with their associated costs in terms of primary losses (e.g., incident response). Additionally, it helps assess the potential number of secondary loss events and the corresponding cost in secondary losses (e.g., legal expenses).

By aggregating these events and their respective losses, an estimated level of risk can be derived.

To define the risk within the simulation platform for the variables of the FAIR model (the FAIR model is described in Section 3.4.4), the aforementioned formula is evaluated numerous times. This involves using different inputs drawn from the selected

distributions. Through the Monte Carlo simulation, a wide range of possible outcomes in monetary terms is obtained, along with their relative probabilities.

3.4.3.2 FAIR-U Risk Analysis Tool

FAIR-U is a free web application for running FAIR risk analysis, offered by RiskLens, the FAIR institute's technical advisor. FAIR-U is used to visualise the likelihood of the loss exceeding a specific threshold using a Loss Exceedance Chart (LEC) methodology. LECs present the outcomes (in the form of a loss exceedance curve or exceedance probability curve) derived from applying Monte Carlo simulations to FAIR risk analysis (Smith, 2020).

FAIR-U is licensed for non-commercial use. Universities can license it for free to use as part of their curriculum. Figure 3.14 provides an example of how Annulised Loss Exposure (ALE) is plotted in the FAIR-U interface.

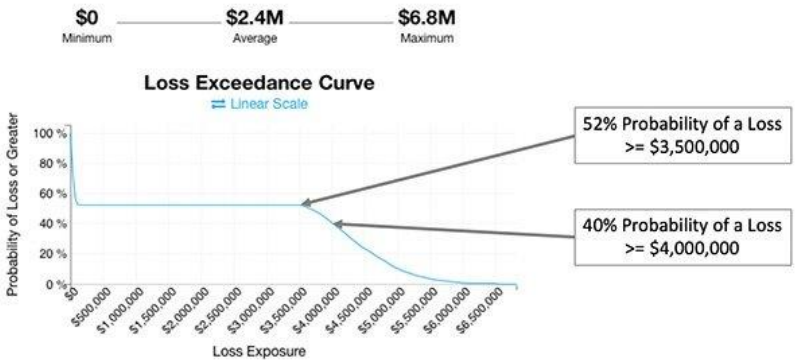


Figure 3.14: Annualised Loss Exposure Example (Smith, 2020)

It also shows a graph where the X-axis represents the ALE for the specific risk scenario analysed, and the Y-axis represents the probability of a loss exceeding the intersection with the X-axis, ranging from 0 to 100%.

Using the outcomes of the Monte Carlo simulations, the FAIR-U tool determines the Probability of Loss by examining the distribution of results and calculating the percentage values that are equal to or greater than segments within the range. Figure 3.14 represents ALE ranging from $0 and $6.8M. As decision-makers, organisations can leverage this data to make well-informed plans. The LECs serve as a guide for organisations to evaluate their comfort level with the potential loss of value and aid in decision-making processes.

To initiate the assessment, consider posing questions like "***Does the organisation's cyber security insurance covers incidents up to $3.5M? What is the***

likelihood of the loss exceeding that amount?" By referring to the LEC, a risk analyst can promptly determine that the probability is 52%. Does the organisation find a 50/50 probability acceptable regarding loss surpassing $3.5M? While they might be comfortable with this level of risk, what if a higher threshold is considered? For instance, what about a loss exceeding $4M? Organisational comfort levels may diminish when faced with such a substantial amount. In this case, the probability stands at 40%. Would the organisation be uncomfortable if there was a 2 in 5 chance of losses exceeding $4M?

This tool enables organisations to determine their level of comfort with potential losses (or risk appetite or acceptance criteria) in a given risk scenario. If an organisation finds the level and probability of loss to be uncomfortable, it serves as an indication that is is necessary to implement, then they create risk remediation strategies to reduce their exposure.

3.4.3.3 Archi Modelling Tool

ArchiMate 3.1 is a modelling language that operates independently and openly, offering a comprehensive set of concepts to assist organizations in implementing Enterprise Architecture (Group, 2019). Archi, on the other hand, is a freely available, open-source, and cross-platform tool designed for creating an ArchiMate 3.1 metamodel. This tool has gained significant adaptation in both the commercial and educational sectors, effectively supporting real-world applications. Archi supports the latest version of the ArchiMate 3.1 language and has a friendly-user interface as depicted in Figure 3.15 (Archi, 2022). In this research, the Archi tool is used to create the connections between concepts in the improved Artefact 2 and Artefact 3.

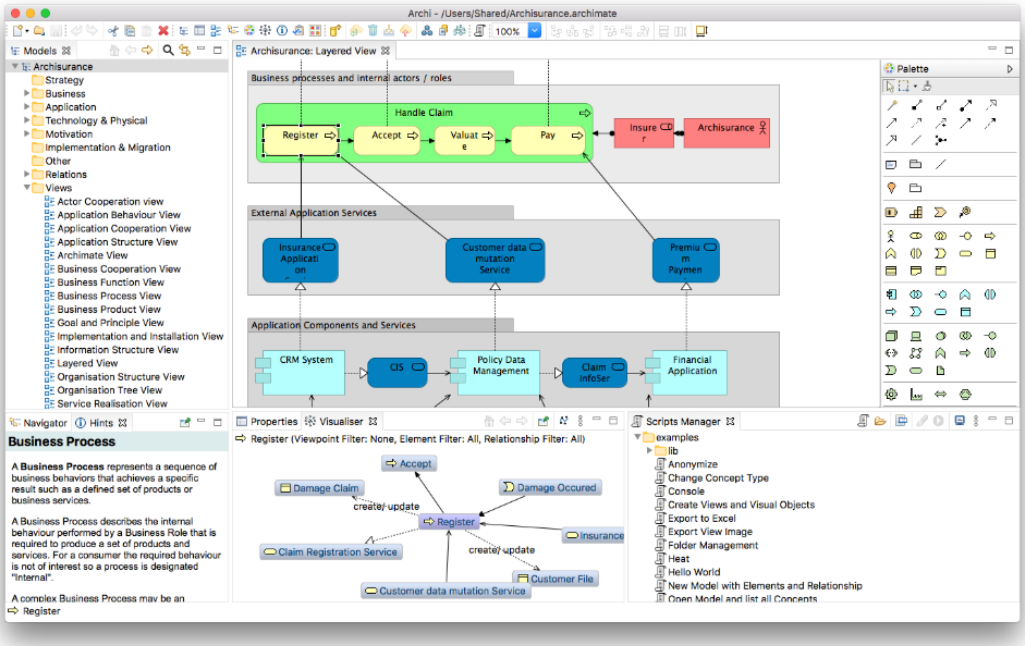


Figure 3.15: Archi Tool Interface (Archi, 2022)

The ArchiMate 3.1 full framework is divided into Layers and Aspects. Figure 3.16 depicts the framework's elements, including the passive structures, behavioural elements, active structures, and motivation. When combined with the six layers, those aspects form a comprehensive framework comprising a total of 24 cells.

The motivational aspect pertains to the interests, motivations, and project goals of an organisation's stakeholders. It involves analysing the outcomes and evaluations while identifying their requirements, principles, and constraints. In the strategic layer, the organisation's action plans, capabilities, and resources are outlined. The business layer encompasses all functions, services, and processes necessary for delivering products within the organisation. The application layer covers all systems, functions, processes, and services employed within the organisation. The technological layer mapps out the organisation's technology landscape. Lastly, the physical layer consists of the infrastructure project of the organisation as a whole (Group, 2019).

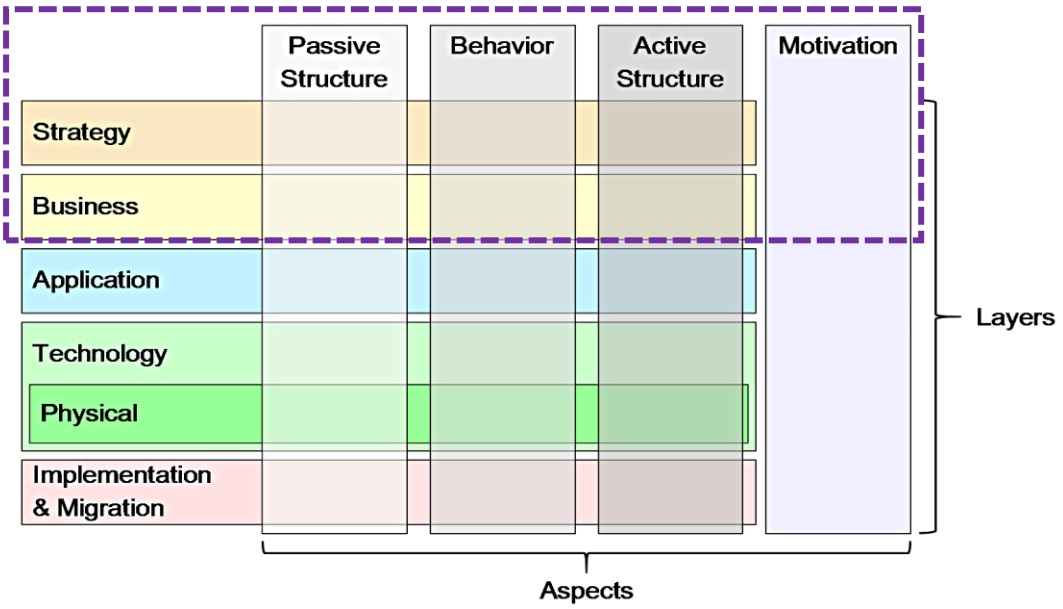


Figure 3.16: ArchiMate 3.1 Full Framework Layers and Aspects (Group, 2019, p. 9)

In this research, only strategy and business layers are considered when designing and modelling the intended Artefact and covering all four aspects in the ArchiMate 3.1 framework, as depicted in the dashed lines in Figure 3.16.

3.4.4 Quantification of Risk

Utilising a quantitative risk approach is vital for making an effective decision to reduce risks. The Factor Analysis of Information Risk (FAIR) is widely recognised as a leading method for performing a quantitative risk assessment. It categorises risk into measurable factors and employs statistical approximation methods such as Monte Carlo simulation, to quantify and estimate the risk (Wang et al., 2020).

The FAIR model translates the impact of identified risk into financial terms. This enables organisations to prioritise security risk effectively, make trade-offs, calculate the Return on Investment (ROI) of security investments, and choose cost-effective solutions to reduce the identified risk. Moreover, the FAIR model helps organisations in addressing critical questions (O'Reilly, 2019) including the following:

- Identifying the organisation's most significant security risks and determining their level of exposure.
- Identifying the security risk management investments that hold the highest importance.
- Evaluating whether the organisation's investment in security risk management is adequate or excessive.

The FAIR model differs from a compliance or risk management framework like NIST and ISO/IEC 27001, as it does not provide a checklist of controls or best practices. Instead, these frameworks are used to evaluate an organisation's adherence to industry standards and best practices. However, they can be used in conjunction with the FAIR model to measure the potential loss exposure resulting from identified weaknesses. In this way, the FAIR model complements these frameworks by enabling organisations to assess the impact or significance of identified and proposed improvements (Jones, 2019).

The rationale behind selecting a FAIR as the suitable method for estimating the risk is that the FAIR model (Freund & Jones, 2014) offers the following benefits:

- Representing clear relationships between each component of this model provides a foundational understanding of risk.
- Providing various techniques for assessing the variables that influence risk.
- Utilising a computational engine that calculates risk by simulating the mathematical relationships between the measured factors in a Monte Carol simulation.
- Relying on a scenario modelling framework that empowers risk analysts to utilise the components, measurements, and computational engine to construct and analyse risk scenarios of virtually any scale or degree of complexity.

In the FAIR model, the risk is a quantity. It represents the anticipated level of future loss resulting from a specific scenario within a defined timeframe. This estimation is derived from assessing the probable frequency and probable magnitude of potential loss events. Thus, analysing risk does not mean rating or scoring but is an act of forecasting that requires an accurate model and valid inputs.

3.4.4.1 FAIR Model Ontology

The FAIR model is best described as an ontology that explains the relationship between various components. This model illustrates the functioning of risk by explaining the factors that constitute a risk and how they are interconnected. These connections can be mathematically expressed, enabling risk analysts to compute risk based on measurements and estimates of those risk factors (Freund & Jones, 2014).

The complete FAIR model ontology consists of two primary branches: Loss Event Frequency and Loss Magnitude. These branches encapsulate the factors that influence

both the occurrence and magnitude of losses. Figure 3.17 presents the high-level abstractions of the FAIR model (Group, 2013).

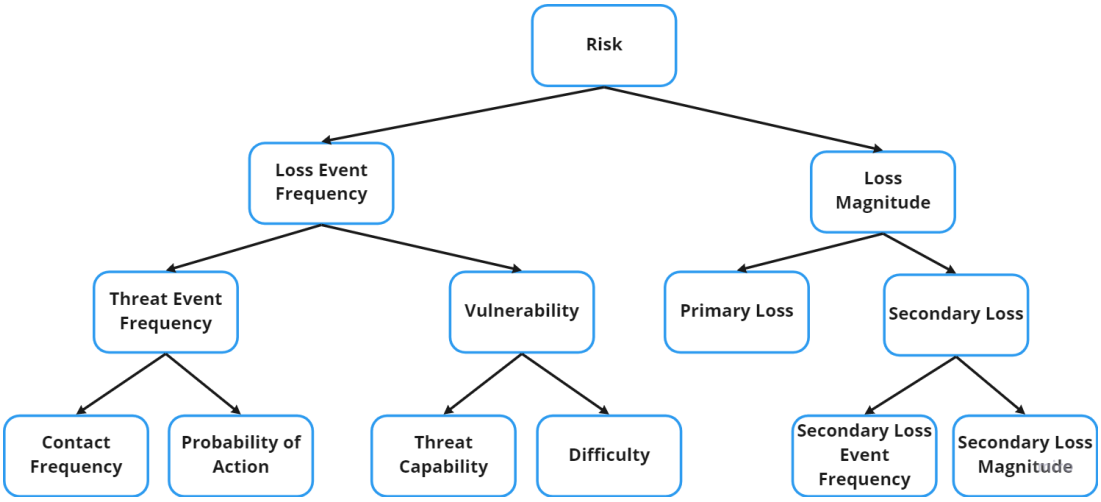


Figure 3.17: Standard FAIR Model Ontology

First of all, the FAIR ontology commences by establishing the notion that risk corresponds to Loss Exposure. Building upon this foundation, the FAIR model defines risk as the likely occurrence frequency and probable magnitude of future loss. Based on this starting point, the initial two factors become clear: Loss Event Frequency (LEF) and Loss Magnitude (LM), which represent the FAIR model top-level ontology. LEF denotes the anticipated probable frequency, within a specific timeframe, at which loss will materialise due to the actions of a threat agent, while LM denotes the probable magnitude of primary and secondary loss resulting from an event (Freund & Jones, 2014).

Secondly, the middle-level ontology decomposes the LEF on the left side into two components: Threat Event Frequency (TEF) and Vulnerability (Vuln); and the LM on the right side into two components: Primary Loss (PL) and Secondary Loss (SL). The TEF denotes the anticipated probable frequency, within a specific timeframe, of threat agents engaging in actions that could lead to a loss while the Vuln denotes the probability that the action of a threat agent will lead to a loss. The difference between PL and SL is that PL is related to the primary stakeholder loss that materialises directly as a result of the event whereas SL centres around the exposure of the primary stakeholder to potential reactions from secondary stakeholder triggered by the primary event (Freund & Jones, 2014).

Thirdly, the lower-level ontology decomposes the middle level into two components each except the PL (i.e., PL is not decomposed). The TEF has two factors: Contact Frequency (CF) and Probability of Action (PoA). The CF represents the probable

frequency, within a specific timeframe, of threat agents coming into a contract with assets while the PoA examines the probability that a threat agent will take acting upon an asset once contact has been established. Similarly, the Vuln is derived from two components: the Threat Capability (TC) of a threat agent and the Difficulty (Diff) level that a threat agent must overcome. On the other hand, the factors influencing the SL consist of Secondary Loss Event Frequency (SLEF) and Secondary Loss Magnitude (SLM). SLEF quantifies the percentage of primary events that resulted in secondary effects while the SLM presents the magnitude of loss associated with secondary stakeholder reactions (Freund & Jones, 2014).

3.4.4.2 Collecting Data and Estimates

The first step in collecting estimates to calculate the risk is to define a set of questions that need to be answered. Those questions represent the variables of the FAIR model and how the forecasts are constructed as illustrated in Figure 3.18.

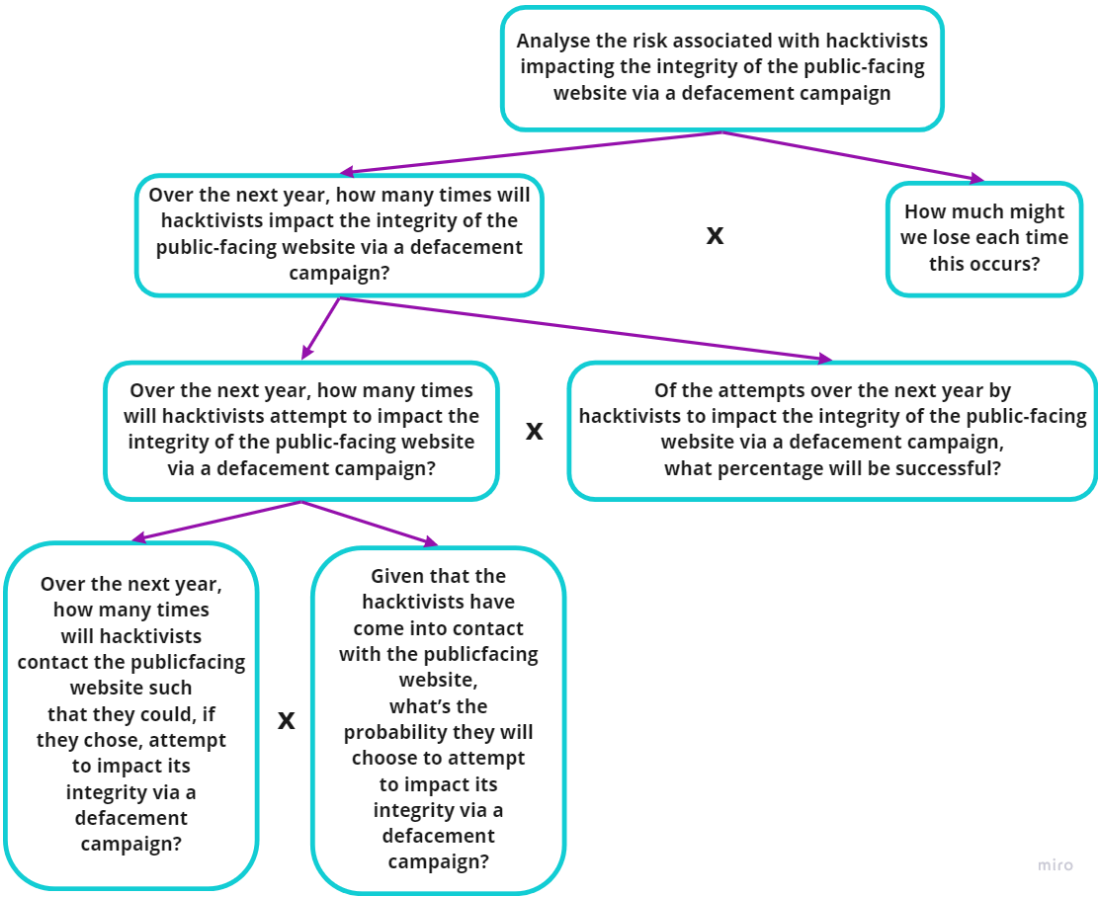


Figure 3.18: FAIR Data Collection and Estimates Example (RiskLens, 2020, p. 33)

Once the variables have been identified, the risk analysts can start to look for data that will allow them to make estimates of these factors.

3.4.4.3 FAIR Model and Proposed Framework Integration

The proposed framework is fundamentally process-driven, comprised of activities that convert input information into desired outputs. Thus, an activity cannot be carried out until all necessary inputs are accessible. On the other hand, the FAIR model breaks down the risk calculation into its constituent components, influencing the sequence of activities. Additionally, a sequence of activities is influenced by the interconnected relationships among the various components of the FAIR model, as illustrated in Figure 3.19 (Group, 2010).

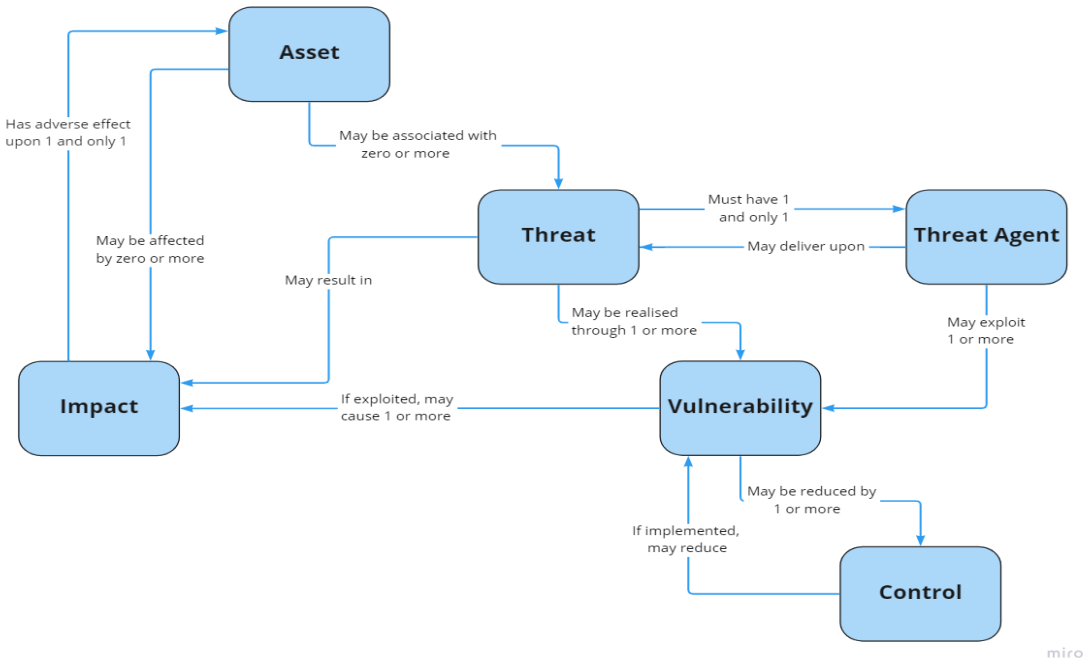


Figure 3.19: FAIR and Proposed Framework Relationships (Group, 2010, p. 20)

Figure 3.20 presents how the FAIR model can be integrated into the Risk Estimation phase within the proposed risk management framework.

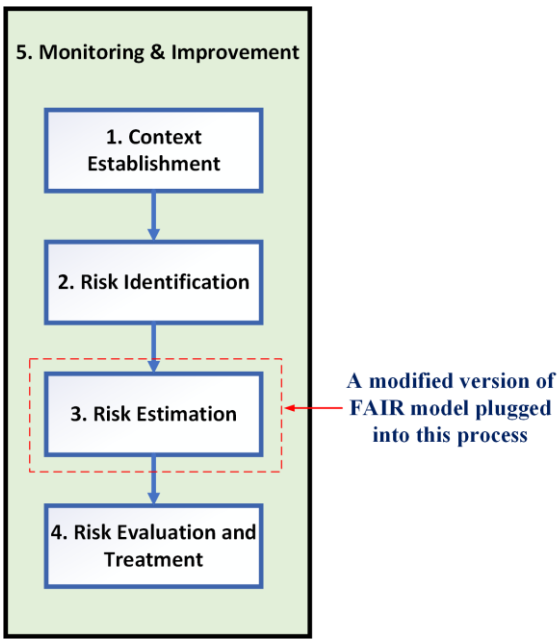


Figure 3.20: How FAIR Model Plugged into a Risk Estimation Process

The researcher develops a more flexible alternative approach that is embedded within the proposed risk management framework. The researcher shows how to reconcile the FAIR model terminology and activities to cover the risk estimation process to create a consistent and repeatable risk management framework. The estimation of risk using the FAIR model allows the utilisation of data/estimates at broader levels of abstraction within the model (e.g., measuring TEF rather than attempting to measure CF and PoA). The flexibility inherent in the FAIR model allows risk analysts to select the suitable level of analysis depending on factors such as time constraints, available data, complexity, and the significance of the scenario at hand (Group, 2010).

It is important to emphasise here that the FAIR model may not provide sufficient details about how the identified risk can be treated. Thus, an adopted and adapted version of the FAIR model has been created to cater for the proposed risk management framework requirements as illustrated in Figure 3.21.

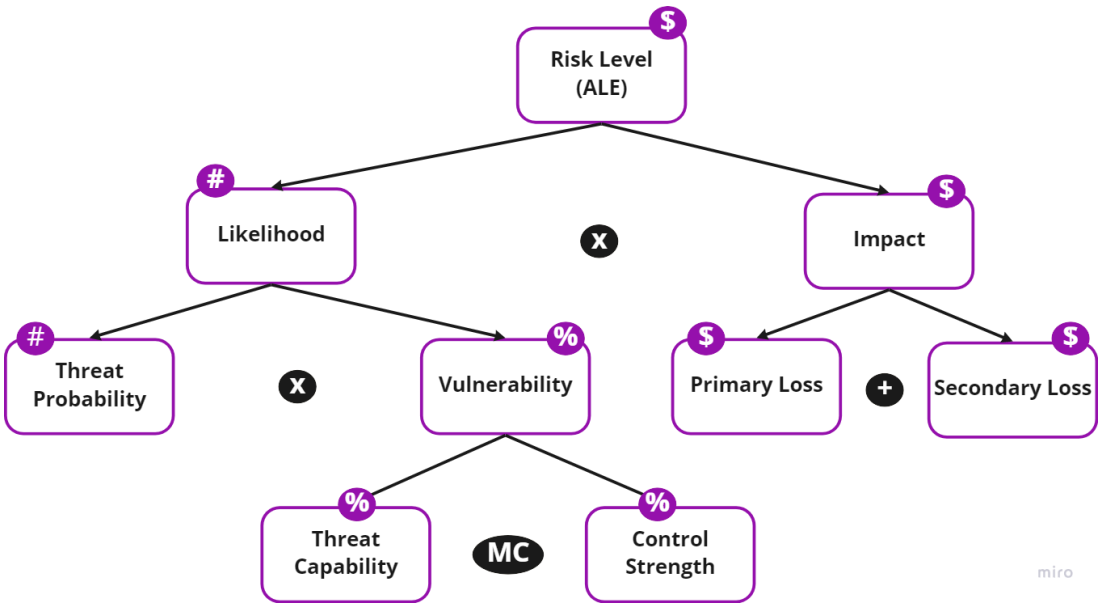


Figure 3.21: A Modified Version of the FAIR Model

The modified version of the FAIR model focuses on the top level and middle level of the standard FAIR model. In the lower level, only two components: Threat Capability and Control Strength were considered to estimate the Vulnerability. The rationale is that the Vulnerability percentage can vary from scenario to scenario depending on the threat agent's capability and the effectiveness of the controls implemented.

New terminologies are introduced to fit the proposed risk management framework ontology. They are more aligned with terminologies found in the industry and international best practices. For instance, Loss Magnitude is replaced by Impact, Loss Event Frequency is replaced by Likelihood, and Threat Event Frequency is replaced by Threat Probability. The Vulnerability, Primary Loss, and Secondary Loss are not changed. However, Contact Frequency, Probability of Action, Secondary Loss Event Frequency, and Secondary Loss Magnitude are omitted as they may produce complexity when attempting to estimate the overall ALE.

3.4.5 Forms of Loss

The FAIR model looks at the losses from two different aspects: primary and secondary. Primary losses are losses incurred by the organisation directly because of the loss event occurring. They are referred to as Primary because the organisation impacted is the primary stakeholder. It is not related to secondary stakeholder reactions such as lost revenue from operational outages, wages paid to employees during non-productive periods due to an outage, replacement of tangible assets (e.g., cash) of the organisation,

and the amount of time and effort invested in restoring functionality to assets or operations after an event occurred (Freund & Jones, 2014).

On the other hand, secondary losses are losses incurred by the primary stakeholder because of the reactions of secondary stakeholders. They are referred to as Secondary because they represent the actions and reactions of secondary stakeholders such as customers, the media, government agencies, regulatory bodies, and contractual third parties (Freund & Jones, 2014). It is worth mentioning here that the FAIR model employs a distinct approach from other methods by not relying on asset value for impact calculation. Instead, it uses Consequences as one of the main components. The FAIR loss forms offer a structured framework to effectively estimate and encompass diverse costs, allocating them to different risk scenarios (Freund & Jones, 2014). In general, FAIR defines six loss forms, which can be observed in both the primary and secondary loss flows: productivity, response, replacement, competitive advantage, fines and judgments, and reputation as described in Table 3.4. It is noteworthy that productivity and replacement costs predominantly occur as a primary loss, whereas the latter three materialise primarily as a secondary loss. However, response losses commonly appear in both primary and secondary loss contexts. Nevertheless, this serves as a general guiding principle.

Table 3.4: Forms of Loss and their Description (Group, 2010, p. 18)

Form of Loss	**Description**
Productivity	The reduction in an organisation's ability to generate its primary value proposition (e.g., income, goods, services).
Response	Expenses associated with managing a loss event (e.g., internal, or external person-hours, logistical expenses).
Replacement	The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop).
Competitive Advantage	Losses are associated with a diminished competitive advantage. This loss is specifically associated with assets that provide competitive differentiation between the organisation and its competition (e.g., trade secrets, mergers, and acquisition plans).
Fines/Judgments	Legal or regulatory actions levied against an organisation. Note that this includes a bail for any organisation members who are arrested.

Reputation	Losses associated with an external perception that an organisation's value proposition is reduced, or leadership is incompetent, criminal, or unethical.

3.5 DESIGN OF ARTEFACT 1

A theoretical framework is a collection of theories and models generated from positivist or interpretive studies of the literature (Collis & Hussey, 2021). The core security risk management is split into two formal processes: identification and treatment. The first one involves identifying and assessing a potential risk (risk analysis), followed by the creation of methods to manage the identified risk (Schneider, 2010). However, establishing organisational context, monitoring, and reviewing continual improvement, and reporting the risk are considered the pre-risk assessment and post-risk assessment requirements. In this section, a conceptual model is introduced to describe the proposed model components.

3.5.2 Artefact Design and Architecture

The proposed conceptual model is based on a combination of both ISO/IEC 31000 and ISO/IEC 27005 frameworks presented in the literature review with some adjustments (e.g., restructuring the framework as required). The key objective of the conceptual proposal is to utilise the evaluated frameworks together in a complementary manner to establish the foundation of a customised security risk management framework.

The proposed theoretical model aims to fill the gaps identified in Chapter 2 in the current ISO/IEC 27050 standard. In other words, it addresses the missing tasks, activities, or processes within the referenced and evaluated risk management frameworks. For instance, key risk indicators and stakeholder analysis are not addressed as part of the risk identification process within the ISO/IEC 27005 standard. In addition to that, the RMF is a threat-centric method that does not address asset identification and evaluation processes as well as stakeholder assessments. Moreover, the Risk IT does not address tasks/activities related to threat and control assessment as part of the risk identification process.

The analysis of the literature in Chapter 2 allows the construction of a draft framework to address the missing risk elements. The structure of the proposed framework consists of three building blocks: principles, framework style, processes, and their relationship. The following sections elaborate on the theoretical framework design.

3.5.2.1 Building Block 1 – Principles

The key benefit of the proposed model is to create and protect organisations' value which then contributes towards achieving the overall organisation objectives. The principles listed in Table 3.5 provide guidance and a foundation for enabling organisations to manage their risk. Moreover, they represent inputs (requirements) when establishing a security risk management framework and its relevant processes. These principles are adopted and adapted from the ISO/IEC 31000 standard.

Table 3.5: Risk Management Principles

No.	Principle	Description
1	Protection	Create and protect organisation value.
2	Integration	Integrate and embed risk activities within all organisation activities.
3	Systematic	Build a structured, comprehensive, and systematic method of risk management.
4	Alignment	Customise risk management framework and its processes according to organisation objectives (e.g., external, and internal needs).
5	Responsibility	Involve related stakeholders as early as possible.
6	Capability	Ensure the risk management can be dynamic, iterative, and responsive to change
7	Quantitative	Consider all historical, and current information and future expectations.
8	Human Behaviour	Consider human and cultural factors.
9	Continual Improvement	Facilities' continual improvement of risk management.

3.5.2.2 Building Block 2 – Framework

The risk management framework comprises various components that interact with each other and establish the fundamental structure of the overall framework, as presented in Figure 3.22. There are five core components with relevant artefacts. Each component produces an output that is used as an input for the next component.

For example, the risk criteria artefact is the output of the Establishment component that is an input for the Identification component. Similarly, the risk analysis method artefact is the expected outcome of the Identification component which feeds into the Estimate component. Moreover, risk level, risk treatment plan, and process

improvement artefacts are the outcomes of the Estimate, Evaluate and Treat, and Monitor and Improve components respectively.

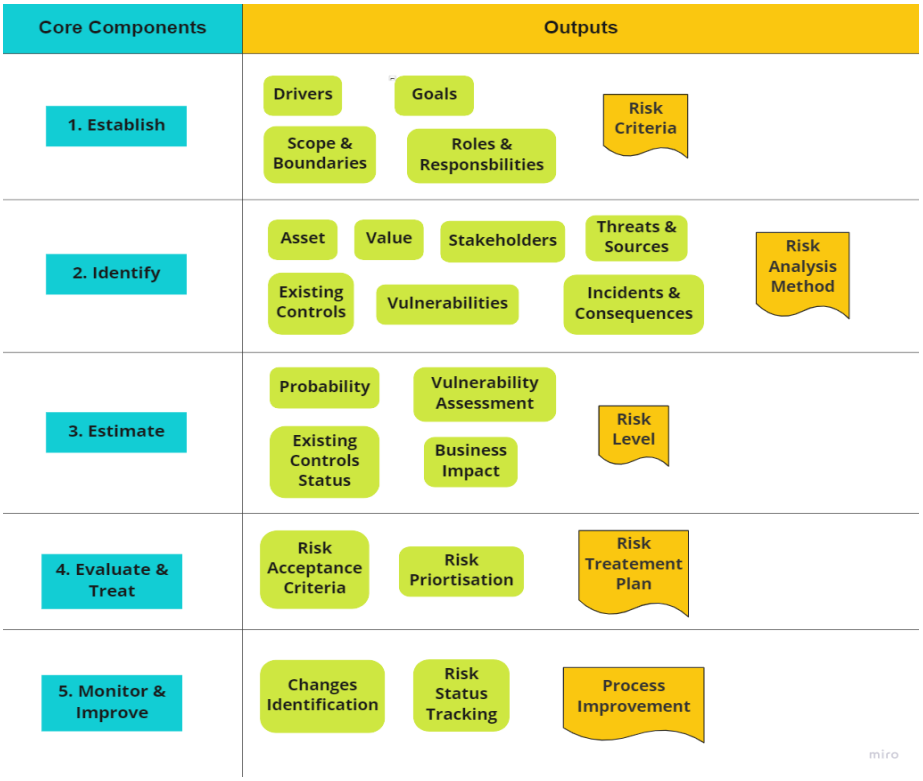


Figure 3.22: Structural Core Components and Relevant Deliverables

3.5.2.3 Building Block 3 – Process

The risk management process consists of a series of actions or steps taken to establish, identify, estimate, evaluate and treat risk as illustrated in Figure 3.23.

The context establishment aims to identify the scope and boundaries and the risk appetite an organisation is willing to accept. It also defines basic criteria necessary for risk management including impact and the acceptable level of risk. This process represents the pre-risk assessment stage. The risk identification identifies relevant stakeholders and defines aspects that could cause a potential loss to an organisation such as threats, vulnerabilities, and incident scenarios. However, a risk analysis method needs to be decided (e.g., either a qualitative, quantitative or a combination of both) before carrying out the risk estimation. The risk estimation determines the impact of the risk, and its likelihood and then calculates the risk level. After estimating the risk, the calculated risk needs to be evaluated before a treatment plan is recommended. The evaluation process includes two important sub-activities: deciding on risk appetite (treat, accept, avoid or transfer), and prioritising the identified risk.

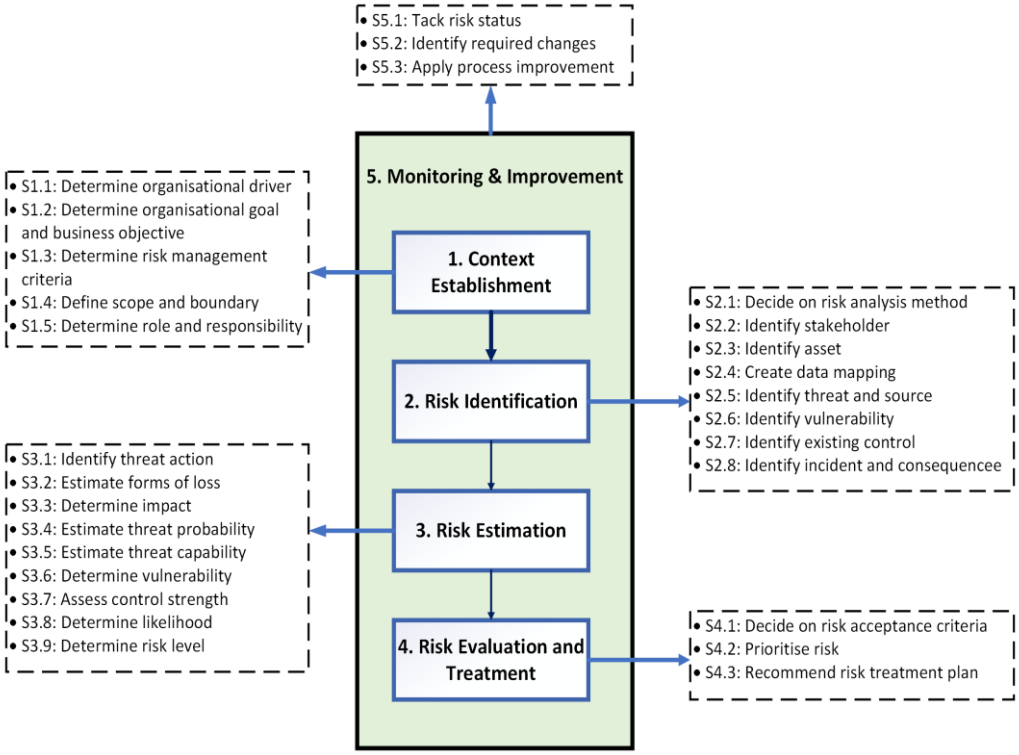


Figure 3.23: Security Risk Management Process

Since the proposed conceptual model is an interactive approach (as discussed in principle 6 and principle 9 in Table 3.5), monitoring and improving the risk management activities become a requirement and represent the post-risk assessment stage. This involves identifying any changes in the context of organisations and maintaining an overview of the complete risk status on an ongoing basis. Furthermore, improving the current risk management activities as necessary and appropriate to the organisations' circumstances.

The process and sub-activities will be detailed in Chapter 4, including the definition of required inputs, actions/steps, and the expected outcome for each process in the context of ESI use cases and scenarios. However, Figure 3.24 illustrates the relationship between the risk management conceptual model elements: principles, framework style, and process; and how they can be adapted or improved to ensure risk management activities are efficient, effective, and consistent.

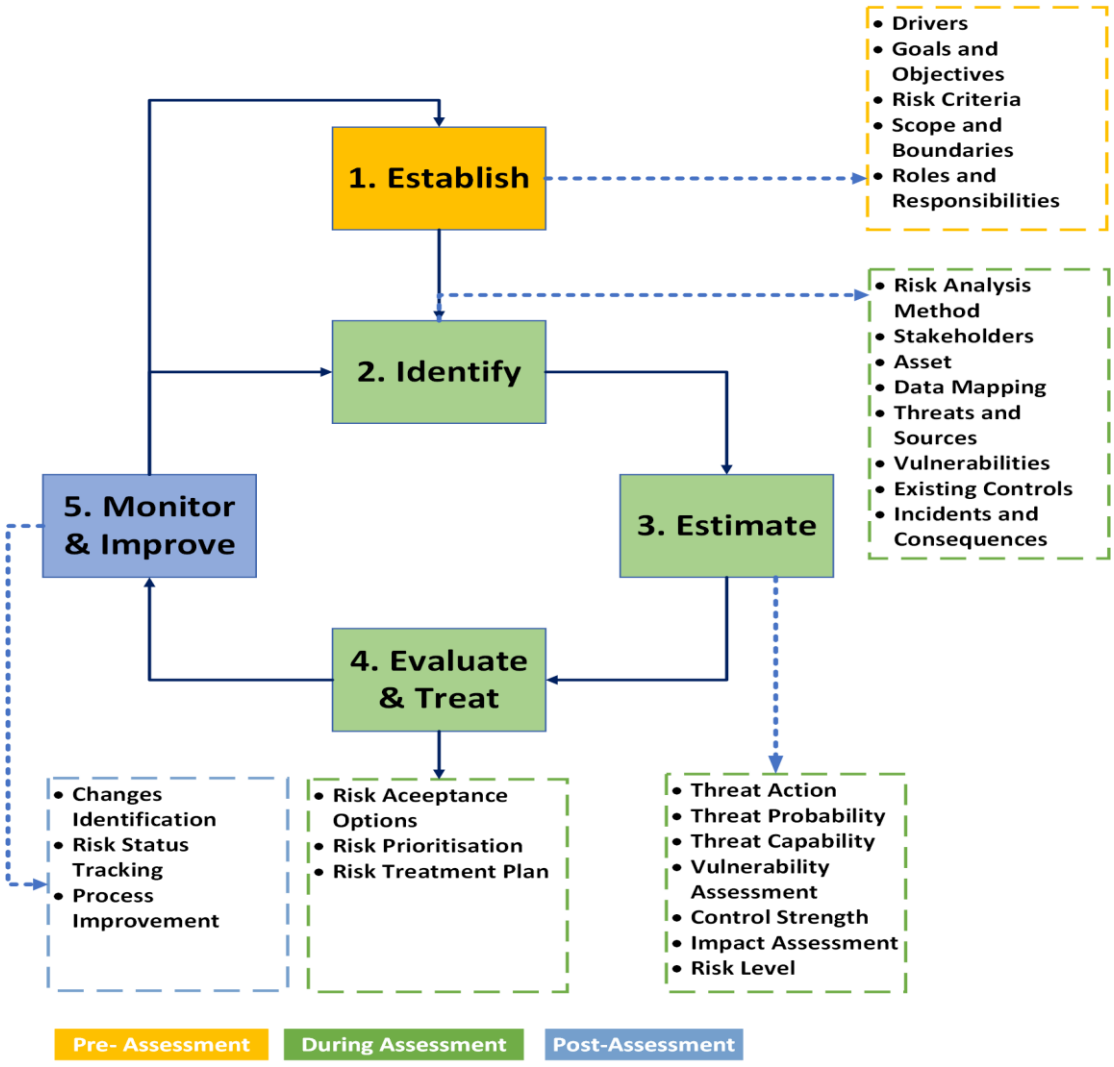


Figure 3.24: Risk Management Principles, Framework Style, and Process and Relationship

3.5.2.4 Constructing a Draft (Strawman) Artefact

The theoretical analysis of the literature has identified the structure and contents of current risk standards and frameworks. The analysis of the ISO/IEC 27050 standard has also provided the scope of eDiscovery and the extent to which risk management is provided. The principles, framework style, and processes described in Section 3.5.2.1, 3.5.2.2, and 3.5.2.3 respectively are now used to construct a draft (strawman) security risk management framework artefact. This artefact will be introduced as the input for a DS development process to improve the design and relevancy for use.

Figure 3.25 shows how the Strawman is used to construct the desired framework artefact. First, the strawman is developed from theory, and then it is tested with three scenarios for improvement.

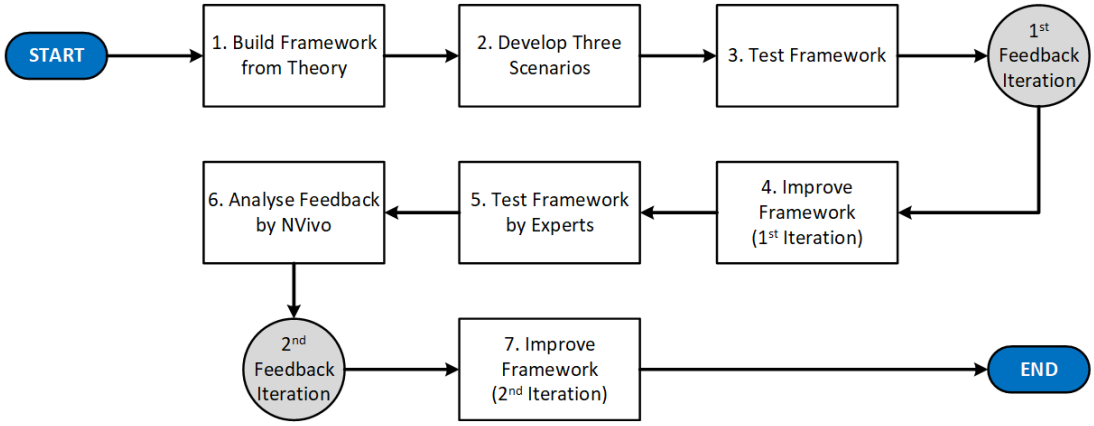


Figure 3.25: Strawman Construction Method

Next, the framework is improved after the first feedback iteration. Then, the improved framework is validated by expert opinion, for the second feedback iteration. The design of the framework is submitted to a group of experts who can envision how the proposed framework will address the research problem and be useful in their work context. The expert opinion does not include any surveys or interviews, but rather the experts are used as a tool to observe and provide both positive and negative opinions of the developed artefact from a feedback template and a brief written introduction by the researcher. The expert feedback is further analysed through the NVivo data analysis tool that has been discussed in Section 3.4.2.4. Then, this feedback is used to improve the framework and remove an inferior, or undesirable component, or add components to the design.

3.5.2.5 Modelling Concepts

The proposed approach includes a set of modelling concepts that are essential to understanding, managing, and expressing security risks. Several concepts have been identified for the development of the security risk management framework. Those concepts are then used to apply the framework for various scenarios as summarised in Table 3.6.

Table 3.6: Modeling Concepts and Descriptions

Concept	Description
Risk	A potential occurrence of an event that may result in the loss, damage, or destruction of an asset due to the exploitation of a vulnerability by a threat, leading to harm to an organisation.

Concept	Description
Driver	Something existing in the organisation that leads to the change like a particular risk could occur.
Scope & Boundary	A holistic risk management insight, constraints, exclusions, and expected results.
Goal & Objective	Achievable outcomes to identify potential risks before occurring and prepare a plan for addressing them.
Risk Criteria	Criteria by which the significance of risks are evaluated, decided, and agreed upon, including the associated cost and benefits, adherence to legal and statutory requirements, consideration of stakeholders' concerns, and setting priorities.
Stakeholder	Any individual or group that can affect, be affected by or perceive itself to be affected by a risk.
Asset	An item of value to an organisation.
Threat	Any entity capable of intentionally or unintentionally taking advantage of a vulnerability, resulting in harm or the destruction of an asset.
Vulnerability	A weakness or gap in control that can be exploited by a threat to damage an asset.
Incident	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of an asset.
Consequence	Positive or negative outcome(s) of an event affecting organisation objectives.
Threat Action	A threat agent acted to target an asset.
Forms of Loss	The monetary impact of a loss for a certain scenario. It is categorised into six forms of loss: Productivity, Response, Replacement, Competitive Advantage, Fines & Judgements, and Reputation.
Control	An attribute that acts as a mitigating factor to minimise risk.
Control Strength	The relative strength of control in comparison to a standard measure of force. Sometimes is it called either Resistance Strength or Difficulty.
Impact	The modelling of the outcome(s) of an event or set of events that can be expressed in a quantitative form.

Concept	Description
Threat Probability	The likelihood of a threat agent taking action against an asset once contact is made.
Likelihood	The expected frequency, within a specific timeframe, of a threat agent acting against an asset.
Threat Capability	The anticipated level of force that a threat agent can apply to an asset.

Through an examination of the concepts within the proposed model, including the attributes of each element and their interrelationships within a real organisational context, the researcher can gain a comprehensive understanding of the existing state of information risk management practices. This analysis enables the identification of potential challenges that need to be addressed in future research.

3.5.3 Artefact 1

Figure 3.26 presents the draft security risk management framework artefact and illustrates the relationship between the components of the risk management conceptual model: principles, framework and process. It also demonstrates how the framework can be adapted or improved to ensure efficient, effective, and consistent risk management activities. However, the model and the relevant processes and sub-activities will be explained as part of the detailed design, including the definition of required input, actions/steps, and expected outcomes for each process in the context of ESI use cases and scenarios in Chapter 4.

The following sections briefly explain the main phases addressed in the proposed framework.

3.5.3.1 Phase 1 – Context Establishment

The first activity begins with collecting information about the target organisation, including its business drivers, goals, and objectives as well as the key roles and responsibilities in the context of security protection. This information helps in defining the required scope and boundaries. A defined scope ensures that all relevant assets are included in the risk assessment process, encompassing identification, estimation, and evaluation. The boundaries establish the specific aspects of the environment or scenario that will be addressed, and the organisation must establish its risk criteria before initiating the risk assessment process.

3.5.3.2 Phase 2 – Risk Identification

Once the scope and risk criteria have been defined, the risk identification will commence. First, the risk analysis method (e.g., qualitative, quantitative, or hybrid) will be selected to conduct the identification process. The risk analyst needs to socialise and engage with the relevant stakeholders (i.e., the asset owners) to identify assets to be protected and threat sources that might pose harm to those assets. To avoid unnecessary costs and efforts, existing controls will be identified. Current vulnerabilities exposed by the threats will be discovered. Lastly, the discovered vulnerabilities will be utilised to create various incidents and consequences scenarios.

3.5.3.3 Phase 3 – Risk Estimation

To estimate risks, it is possible to use either a qualitative or quantitative approach (as selected previously) to assess threat probability, vulnerability, and business impact, and then evaluate the existing controls. For each identified consequence scenario, a specific value will be determined. The probability of each incident potentially affecting an asset and resulting in consequences will be assessed. To calculate the risk level, the assigned values for threat, vulnerability, impact, and control effectiveness will be computed using a risk level formula.

3.5.3.4 Phase 4 – Risk Evaluation and Treatment

Each identified risk will be evaluated based on established risk acceptance criteria. The identified risks will be prioritised along with the controls chosen to reduce the risk to an acceptable level. The results of this evaluation will be documented in a risk treatment plan, which will also identify any residual risks. If the risk treatment plan is not approved by the risk owner, the process will iterate, and further assessments and adjustments will be made until an acceptable plan is achieved.

3.5.3.5 Phase 5 – Monitoring and Improvement

The identified threats, vulnerabilities, business impact, and control effectiveness may change due to changes in the organisation's context (e.g., infrastructure, people, processes, new threat vectors, and risk approach). Organisations must reflect not just the ability of controls to ideally treat the identified risks but also their actual effectiveness in

terms of consistent, comprehensive, reliable, and timely operation. Thus, after documenting the risk treatment plan, continuous monitoring will be conducted to identify any changes that could impact the organisation. This ongoing monitoring ensures that the outcome of the risk assessment and treatment plan remains relevant and suitable for the current circumstances. Any identified changes will be used to improve the overall security risk management process (i.e., they can result in adjusting the current risk approach/methodology).

Table 3.7 shows the mapping and relationship between the nine principles and the five risk management phases.

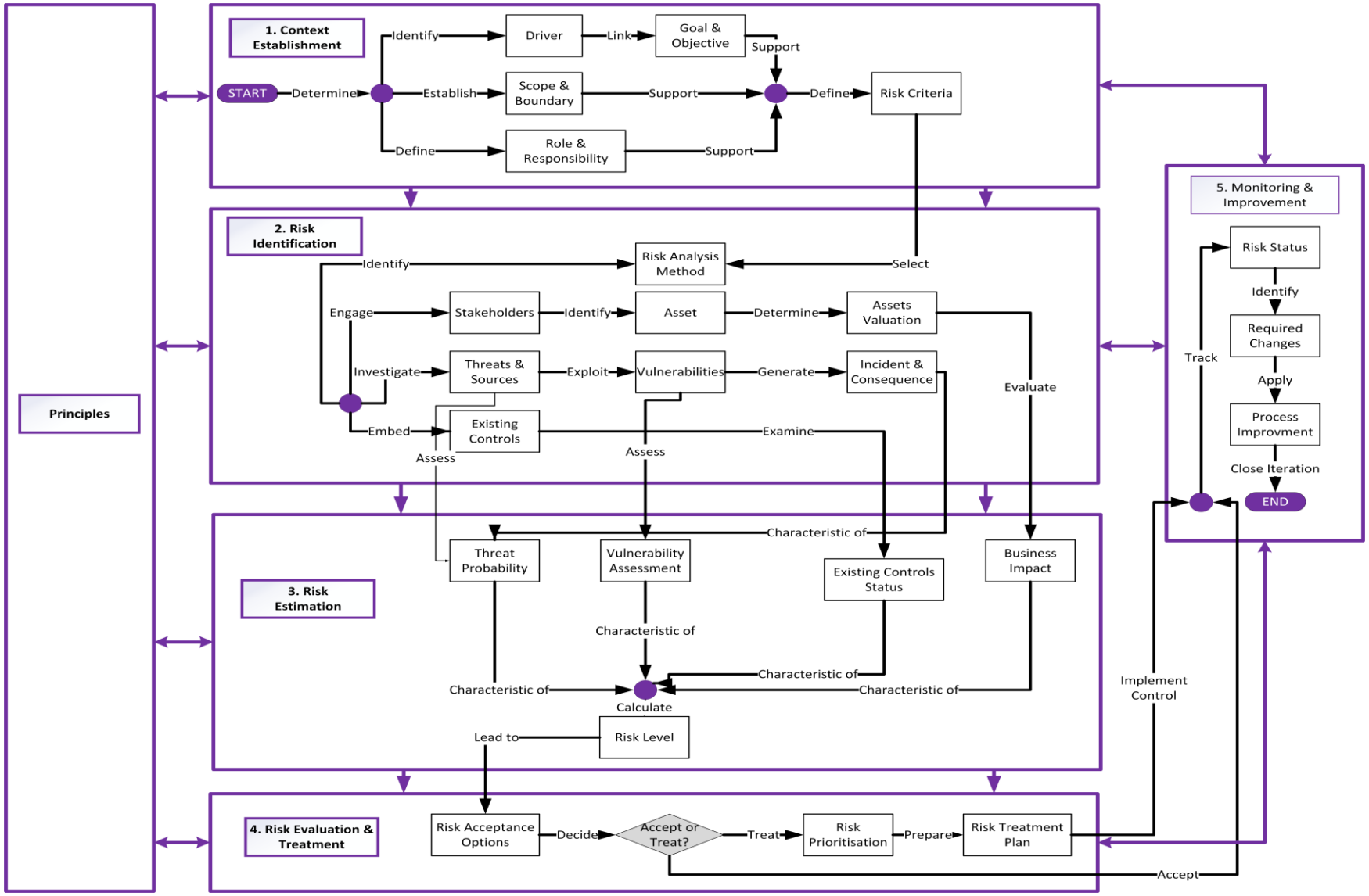


Figure 3.26: Security Risk Management Framework (Artefact 1)

Table 3.7: Principles and Risk Management Process Relationship Mapping

No.	Principle	Risk Management Process				
		Context Establishment	Risk Identification	Risk Estimation	Risk Evalatuion & Tratement	Monitoring & Improvement
1	Create and protect organisation value.	☑				
2	Integrate and embed risk activities with all organisation activities.	☑	☑	☑	☑	☑
3	Build a structured, comprehensive, and systematic method of risk management.		☑	☑	☑	
4	Customise risk management framework and its processes according to organisation objectives (e.g., external, and internal needs).	☑				
5	Involve related stakeholders as early as possible.	☑	☑			
6	Ensure the risk management can be dynamic, iterative, and responsive to change.					☑
7	Consider all historical, current information and future expectations.	☑				
8	Consider human and cultural factors.	☑	☑			
9	Facilities' continual improvement of the risk management.					☑

3.6 LIMITATIONS

Like any other research, the proposed framework has some limitations. This research will not address aspects of risk management beyond risk assessment, monitoring and improvement; and will be limited to activities only related to how to design and conduct risk modelling and including risk establishment, risk assessment (identification, analysis), risk calculation, risk treatment, risk acceptance and improvement. The research does not cover the risk communication and consultation phase as it focuses on understanding that risk communication is an embedded activity involving relevant stakeholders.

During the development of research objectives and the selection of methods, researchers need to take into account the potential impact of validity and reliability on their research (Berndtsson et al., 2008). In this research, Design 1 is derived from theory and possesses identifiable features suitable for scenario testing. Specifically, the proposed framework includes attributes, properties, clusters/groups of entities, and related links. The scenario tests will then produce Design 2 which is a test of the reliability of the framework Design 1 (i.e., that shows improvements). Expert feedback is used for the research validity. It is a reflection on the framework and a final Design 3.

3.6.1 Reliability

Berndtsson et al. (2008) define reliability as the accuracy of the proposed method (e.g., deployment, experts' opinions) in examining or developing a proposed method. Moreover, reliability in research pertains to the consistency of results obtained when the study is replicated. It means that if another research group attempts to conduct the same study using the same procedures, they would obtain similar outcomes. Thus, repeatability plays an important role in ensuring the reliability of research findings.

The testing of hypotheses is crucial for ensuring the reliability of the research results as it provides numerous opportunities to examine and analyse the findings (Berndtsson et al., 2008). In general, reliability focuses on the robustness of the implementation of the proposed method. In other words, it is the internal consistency of the proposed method (i.e., audit, checks, and performance). In this research, the scenario test will be conducted to evaluate the reliability of the proposed method. It will be used to analyse the suitability and utility of the implementation of the scenarios instantiation artefacts. The scenario tests will be evaluated and presented in Chapter 4. Three different scenario tests will be conducted. The Strawman will be applied to each scenario to evaluate its strengths and weaknesses. After presenting the scenario tests, errors and

omissions will be reported to show the difference and improvement between Design 1 and Design 2.

The researcher believes that using scenario tests will be a viable measurement tool to give a degree of assurance to the core features of Design 1 but also acknowledge the limitations and the requirement for improvement and the need to move to the improved Design 2.

3.6.2 Validity

According to Berndtsson et al. (2008), validity is defined as the correspondence between the researcher's intentions and what is examined or developed in a study. It is an important aspect that enhances the applicability of research. Determining validity requires evaluating the proposed artefacts, and ensuring they fulfil the necessary conditions to achieve the desired outcomes (Dresch et al., 2014). Moreover, validity acts as a test to measure precisely what the researcher intends to measure, and the results accurately reflect the phenomenon being studied (Collis & Hussey, 2021).

In the context of this research, validity aims to show that the proposed artefacts are valid by confirming the utility of the proposed artefacts within their field of application. The validation process is conducted using an expert opinion method, wherein a group of designated experts will provide scientific views or comments. This is achieved by conducting a comprehensive review of scientific evidence and/or seeking expert opinions to gather valuable insights and validate the research findings.

Experts are highly suitable for evaluating the proposed artefacts, not only for final assessment but also for conducting interim evaluations that introduce incremental improvements to the proposed artefacts (Dresch et al., 2014). Their expertise and knowledge make them well-equipped to provide insightful feedback and suggestions throughout the development process, ensuring the continuous enhancement and refinement of the proposed artefacts. However, one of the main limitations of this research is the selection of experts for feedback. The selection criteria are based on a subjective assessment of the required competency and experience of the experts participating in the research evaluation. The evaluation of this research is restricted to 10 experts' feedback as it requires arrangement with chosen experts as well as exhaustive efforts for feedback analysis. Data gathered from expert opinion evaluation are analysed and interpreted to support in determining the validity of the proposed artefacts; then apply any necessary changes.

The expert opinion evaluation provides input for the proposed artefact, refinement through an iterative process input to Design 3. This input provides observation, measurement quantification, and confirmation in terms of how well the artefacts output supports the proposed solution to the identified problem (i.e., research questions and hypotheses). The output from the iteration of this process provides information in the form of knowledge that the proposed research is novel. Subsequently, the knowledge will be published and communicated through the release of the research output in the form of a PhD thesis as well as research articles in Journals and research papers in Conferences.

3.7 CONCLUSION

This chapter starts by presenting the concept of DS and describing two well-known methodologies. In DSR, the fundamental principle is that knowledge and understanding of a design problem and its solution are required through the process of developing an artefact. This chapter also presents an adaptive version of two DSR methodologies that have been adopted to meet the research requirements. The goal of this research is to answer the primary question that is "**What framework aligns the current ISO/IEC 27050 standard with the ISO security risk evaluation framework in a cost-effective way?**" by proposing a solution.

The proposed model was developed based on various international standards and selected analysed literature. The structure of the proposed model consists of three building blocks: principles, framework, and processes and their relationships. This model is limited to core risk assessment processes: context establishment, risk identification, risk estimation, risk evaluation and treatment, and finally monitoring and improvement. It does not consider the communication and consultation process as noted. Moreover, the proposed model was constructed and improved using a Strawman method with a set of activities starting from building a framework from theory, developing three scenarios, testing those scenarios, improving Artefact 1, evaluating Artefact 2 by selected experts till introducing the final version of the proposed framework (Artefact 3).

A modified version of the FAIR model has been developed to show how to reconcile the FAIR model terminology and process to cover the Risk Estimation process to create consistent and repeatable risk management framework components. Monte Carol Simulation and FAIR-U tool are used to estimate the risk. Moreover, the Archi tool is used to create an ArchiMate 3.1 metamodel and sketch for the proposed artefact. The proposed framework is focused on activities only related to the design and

implementation of risk management. This includes risk establishment, risk identification, risk analysis, risk calculation, risk treatment, risk acceptance and improvement. In this research, the scenario test is conducted to evaluate the reliability of the proposed method. As part of research validation, an expert opinion method is used to collect feedback on applicability for use.

Finally, this chapter provides the definitive framework (Artefact 1) and starting point for creating the required artefact improvement that is reported in Chapter 4. Therefore, Chapter 4 presents a detailed scenario testing the proposed conceptual model to manage risk and its key components, the steps involved in the risk management processes, flowcharts, inputs, and expected outcomes of each step. The data will review Artefact 2 and an improved framework.

Chapter 4: Artefact 1 Scenario Tests

4.0 INTRODUCTION

Figure 4.1 shows the summary of the thesis structure based on the proposed research methodology. The dashed lines show the roadmap for Chapter 4 which is Phase 4 (Artefact Application Demonstration).

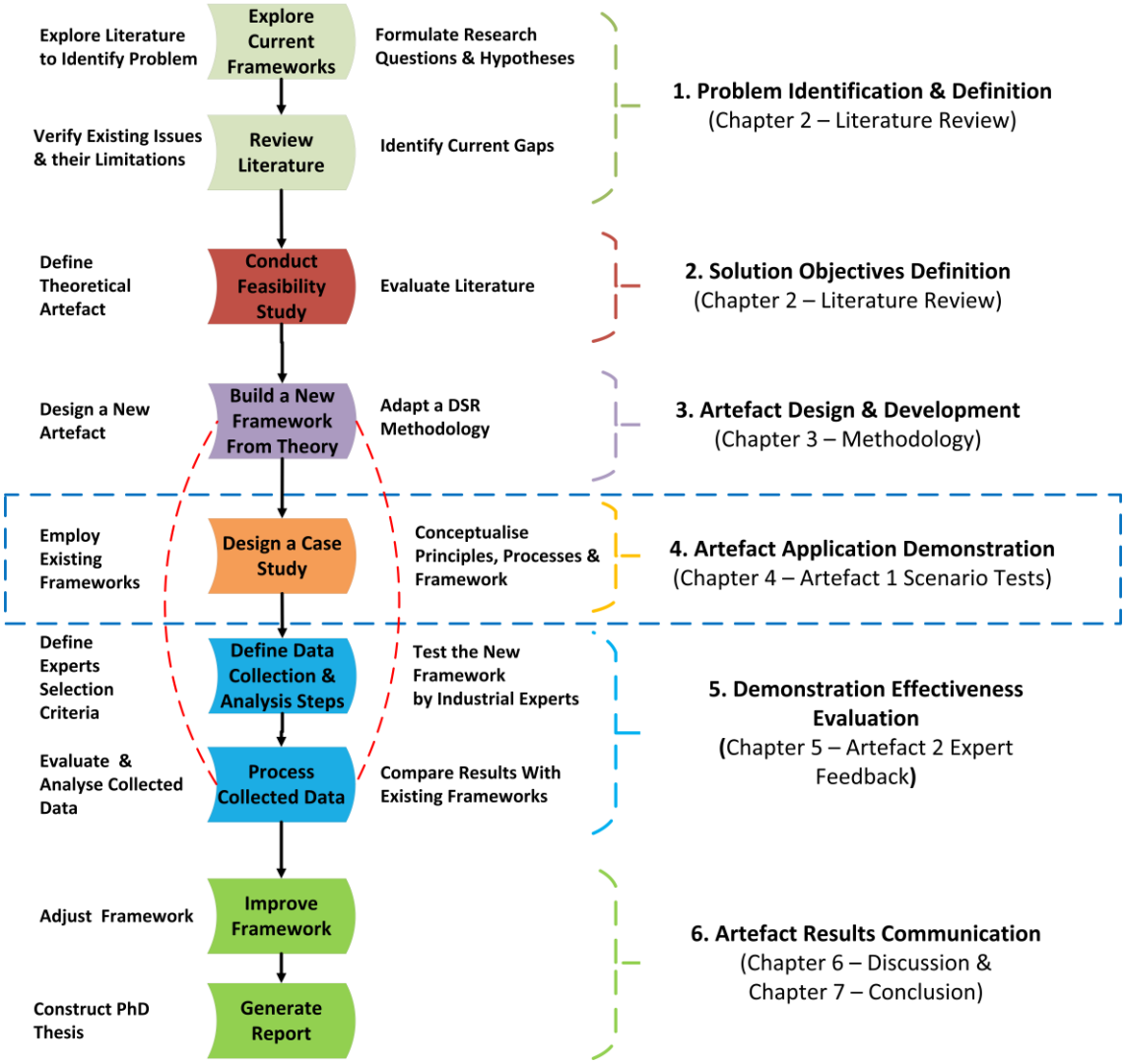


Figure 4.1: Chapter 4 Roadmap

Scenario testing activity uses real stories to help the researcher understand a complex problem, the eDiscovery processes, and the completeness of Artefact 1. In the context of this research, three scenarios are chosen: IT service provider, energy provider, and health service provider. These scenarios represent a variety of eDiscovery cases.

This chapter is structured as follows. Section 4.1 discusses a scenario of an eDiscovery process for searching, locating, and securing electronic data to use as

evidence in a legal case. Section 4.2 presents a scenario of data leakage that organisations face when they store the IP of third parties in multiple locations. Section 4.3 presents a scenario of the implications of inconsistent medical records from a risk perceptive. Each scenario is defined, tested against Artefact 1 framework, and then the results are examined and discussed to identify aspects for improvement in Artefact 1. Section 4.4 presents the recommended changes for the new version of the proposed framework (Artefact 2), and a list of the changes made. This chapter ends with the main conclusions and a connection to Chapter 5 in Section 4.5.

4.1 SCENARIO 1 – COLLECTING ELECTRONIC CONTENT FOR LEGAL CASES

An eDiscovery investigation involves the process of searching, locating, and securing electronic data to use it as evidence in a legal case. In other words, it schedules a repeating search to gather relevant content during the discovery period, indexes the content in a case, flags content of interest, and finally exports content to an industry-standard format for delivery to the legal counsel.

4.1.1 Define Scenario

Electrooze Energy company was formed in 2002 to generate electricity from 80% renewable sources including wind, geothermal, and hydroelectric. Electrooze is a multinational company with headquarter in Texas, United State of America. It has more than 10,000 employees and operates 67 power stations across the globe.

Electrooze faced a variety of challenges related to accessing and sharing sensitive information stored in emails, file servers, and databases. To address these challenges, Electrooze has implemented authentication control to ensure that only authorised users have appropriate access to Electrooze data and to prevent authentication process failures. Additionally, there is a requirement to support litigation efforts, including placing legal holds on data. Managing a substantial volume of information-related storage and complying with regulatory obligations are also important responsibilities for Electrooze.

In the current scenario, Electrooze is facing a lawsuit, which adds complexity to the situation. When anticipating the potential litigation, it is crucial for Electrooze to promptly put a legal hold, which prevents any deletions or revisions to responsive documents. Typically, the lawyer involved in the case will provide a written definition of documents and data to be preserved once a lawsuit is filed. At this stage, Electrooze must halt all deletions or potential overwriting of any responsive data until the case concludes.

It is essential for Electrooze to regularly verify and ensure proper enforcement of the legal hold. Any attempts to destroy evidence while a legal hold is in effect can result in penalties or monetary judgments imposed by the court against the party responsible for such actions (Heikkila, 2008).

4.1.2 Test Artefact 1 Framework

This scenario is tested through the first artefact design for the proposed framework. The next sections show the framework's main phases along with their relevant steps.

4.1.3 Phase 1 – Context Establishment

Electrooze needs to continue with risk mitigation activities and establish robust foundational controls while enabling the business through a proactive approach to security. In particular, Electrooze needs to resolve typical problems with organisation content management and eDiscovery for legal cases.

4.1.3.1 Team Involvement

Electrooze is responsible for the management of large volumes of ESI particularly with litigation, regulation, or any form of dispute or adversarial circumstances involving multiple parties. However, before an information disclosure incident relevant expertise is established in an eDiscovery team with all roles and responsibilities required. This team as a whole is responsible to ensure the smooth running of any eDiscovery process in case of a security breach (ISO, 2020b). The team engaged in this scenario consists of various roles as depicted in Figure 4.2.

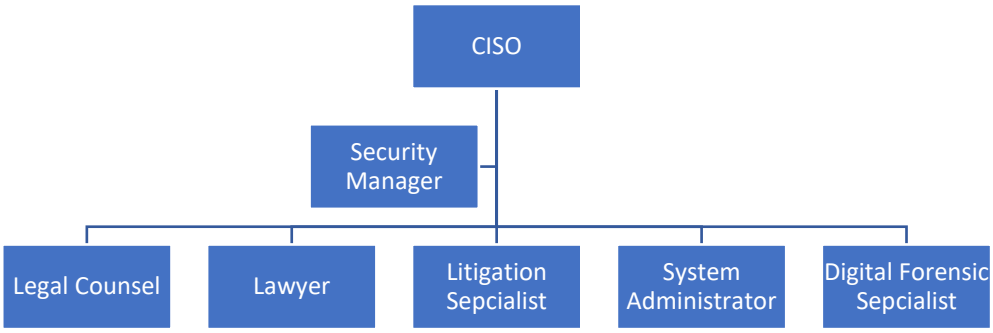


Figure 4.2: Team Engagement in Electronic Discovery Incident

The CISO is responsible for decision-making and rule set for the policies surrounding ESI management, retention, and destruction while the Security Manager oversees the security controls that are in place to meet privacy and data protection requirements.

On the other hand, both System Administrators and Digital Forensic Specialists play an important role in the technology side of the eDiscovery process. The System Administrator has the technical knowledge of the eDiscovery platform and content management platform. The advisory on ESI preservation and collection is part of the Digital Forensic Specialist's responsibility.

The activities related to legal aspects are handled by the Legal Counsel, a specialised Lawyer, and Litigation Specialist. The Legal Counsel is part of the Legal Team, which ensures that legal requirements are identified during the investigation process (e.g., legal privilege, evidence collection, court processes, court orders, and agreements between different parties). The Litigation Specialist plays a key role in providing consultation and supporting services to both Legal Counsel and Lawyers on litigation cases. The Litigation Specialist also supports the System Administrator in managing the eDiscovery platform and performing a regular assessment of that platform.

Electrooze appoints an expert Lawyer who understands the legal implications of an information disclosure incident, especially the implications of using technology-assisted review and how this can be managed and explained in the court of law context.

Three important aspects are described: the ArchiMate 3.1 design, the Data Flow Diagram (DFD), and the Business Process Model (BPM) in the context of this scenario. The ArchiMate 3.1 design presents a clear set of concepts and the relationship between architecture layers, including business, application, technology, and physical, as well as various views. The DFD demonstrates the physical movement of data whereas the BPM concentrates on the logical activities of the actors for an eDiscovery process.

Table 4.2 provides a summary of the Context Establishment steps.

Table 4.1: Summary of Context Establishment Steps

Step	Description
Organisational Drivers	Increasing cyber threats against inadvertent disclosure of sensitive information to outside Electrooze environment.
Organisational Goals and Business Objectives	The Leadership Team wants to ensure better control is in place for sensitive information and resolve issues with Electrooze's content management and eDiscovery for legal cases.
Scope and Boundaries	Electrooze faces a security risk when sensitive information is unintentionally disclosed to outsiders who should not know the content. Therefore, the primary scope is to analyse the risk associated with insiders (e.g., employees, contractors, vendors,

Step	Description
	and business partners) impacting the confidentiality of the content management system via information disclosure.
Key Roles and Responsibilities	Employee creates, process, and store information. System Administrator configures, manages, and maintains servers (email, file, and database) and the eDiscovery system (analyser, manager, and collector). Legal Counsel creates legal cases, searches for appropriate data during the discovery, and places a legal hold on the content that matches the search criteria.
Risk Criteria	Protection - Information must be preserved in its original state and safeguarded against unintentional or deliberate exposure to individuals. Legal Requirements: A court-issued protective order specifies the authorised individuals who can access the data and outlines the appropriate handling procedures for the duration of a legal proceeding.

4.1.3.2 Architectural Modelling Design

The eDiscovery ecosystem consists of three main building blocks: web interface, eDiscovery platform, and content management platform. Each building block has three IT components as illustrated in Figure 4.3.

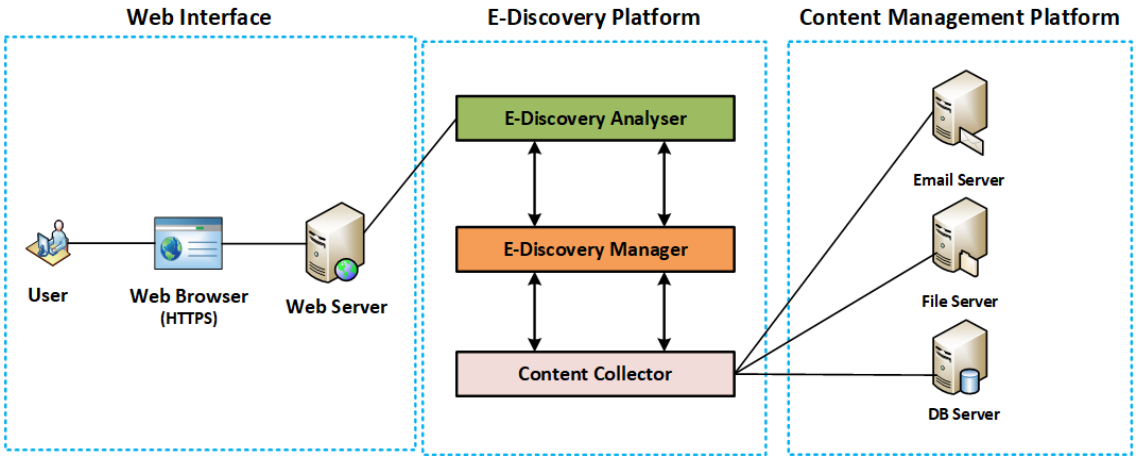


Figure 4.3: Scenario of Electronic Discovery Architecture

To manage data sources and prepare for eDiscovery, Electrooze installs and configures a Content Collector to archive its business content, then uses eDiscovery

Manager to quickly discover data that is potentially relevant to a legal matter and place that data on legal hold to prevent deletion until the matter is resolved. Next, the Legal Counsel uses eDiscovery Analyzer on this drastically reduced set of data to not only better understand its bearing on the legal matter but to quickly distinguish between responsive, non-responsive, and privileged information.

Figure 4.4 presents an architecture design modelling of the eDiscovery based on the ArchiMate 3.1 four layers: Business, Strategy, Application, and Technology layer with three core elements: Active structure, Behaviour structure, and Passive structure element.

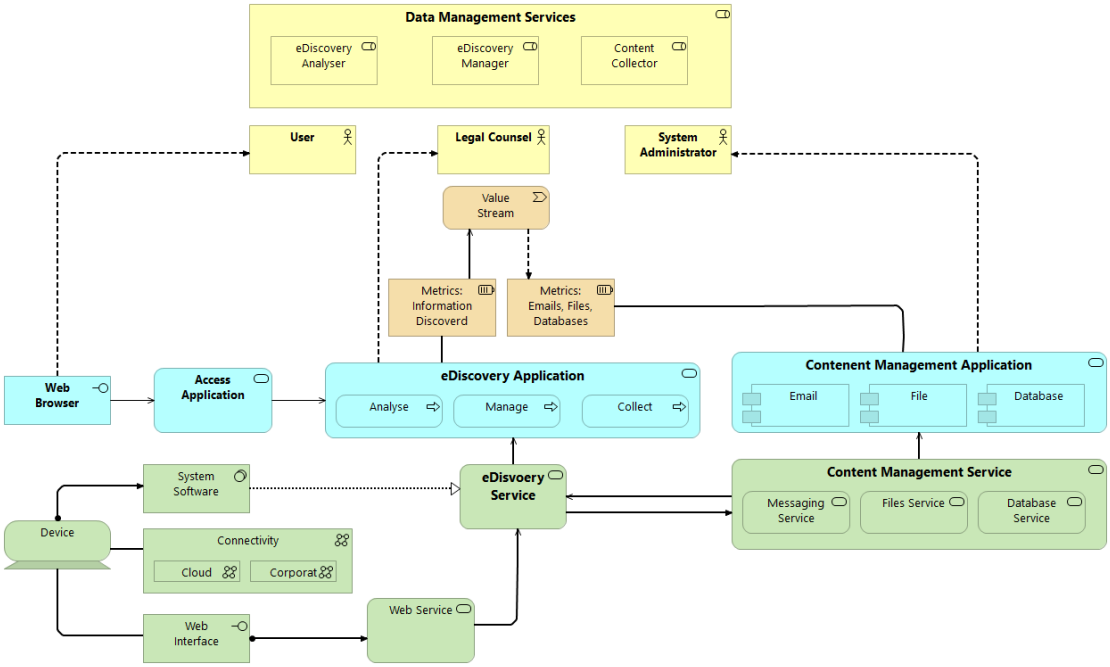


Figure 4.4: Electronic Discovery Architecture Design based on ArchiMate 3.1 Model

4.1.3.3 Data Flow Diagram

The DFD describes the flow of information in the system, tracing its path from external entities to processes and data stores. Through the use of arrows and concise labels, the DFD visually indicates the direction of the data movement. Figure 4.5 provides a contextual map of the eDiscovery process in two directions from the user to the platform and back again as described below:

- A user accesses the eDiscovery platform via a web browser in an encrypted format (HTTPS).
- Then, the web application connects to the eDiscovery Analyser and the eDiscovery Manager exchanges data between the eDiscovery Analyser and

the Content Collector.

- The Content Collector gathers documents and emails from three main sources: an email server, a file server, and a database server.

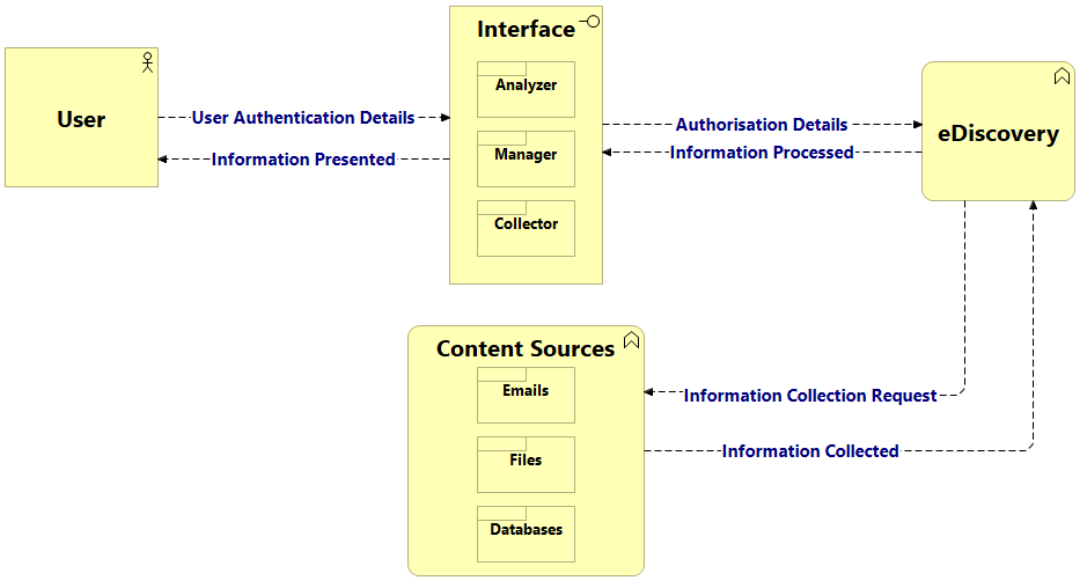


Figure 4.5: Data Follow Diagram for Electronic Discovery Process

4.1.3.4 Business Process Model

eDiscovery offers a systematic workflow for preserving, gathering, analysing, reviewing, and exporting content that is responsive to Electrooze's internal and external investigations. Additionally, it enables the Legal team to effectively handle the entire process of notifying custodians about legal holds associated with a case. In eDiscovery Manager, each case corresponds to a specific legal case, which could be a regulatory inquiry, ongoing litigation, or an internal investigation. A case may contain one or more folders, each containing the documents obtained from one or more search operations.

When Electrooze needs to produce ESI in response to legal proceedings, Electrooze encounters numerous security risks and must adhere to specific legal obligations. The use of the eDiscovery process, technology, and governance play an important role in safeguarding against unintentional disclosure to unauthorised external parties ensuring compliance with organisational and legal requirements. A protective court order identifies unauthorised individuals who can access the content and outlines the appropriate handling procedures throughout the litigation case (Heikkila, 2008).

Figure 4.6 shows a simplified eDiscovery BPM. Electrooze has a large volume of archived emails and other documents. The System Administrator sets up a server that archives email and business documents. In addition, the System Administrator installs

and configures the Content Collector so that the email and business documents can be discovered if required. By using the eDiscovery Manager, the Legal Counsel creates a case and searches for data to identify current content. For business collection, the discovery scope encompasses email addresses, specific date ranges, and targeted search terms applied to the subject, body, and attachments of emails. This approach aims to identify content that may be relevant to the legal matter at hand.

Once the results are determined to be relevant to the eDiscovery process, the Legal Counsel imposes a legal hold on the content. This action automatically locks the content, preventing any alterations or deletions from the server until the litigation process is concluded. The legal hold also ensures all modifications and deletions of responsive content are halted. To provide an additional layer of protection, a separate legal hold repository is established outside Electrooze corporate network. This ensures that the ESI remains intact and secure, safeguarding it against accidental deletion or unauthorised disclosure to individuals who lack proper authorisation.

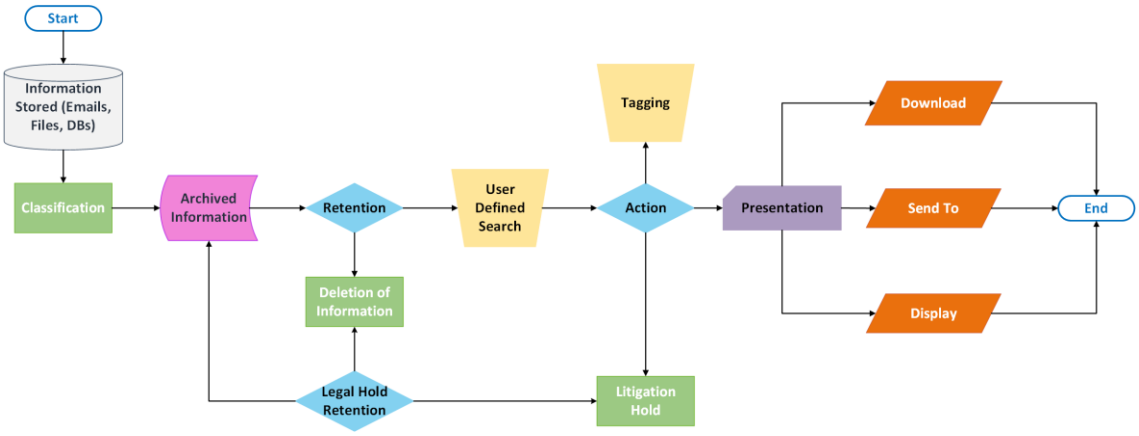


Figure 4.6: Simplified Electronic Discovery Business Process Model

When the search is completed, the Legal Counsel uses the eDiscovery Analyzer to export and transfer the content for further processing (e.g., flagging information is also included in the exported data). The eDiscovery Manager generates an audit report that provides a comprehensive overview of the performed search, including the user responsible for conducting the searches, and a detailed list of the exported content. This report is then securely communicated with the custodians involved in the legal case.

4.1.3.5 Obtaining Valid ESI

Every lawyer realises that some rules and procedures must be followed when obtaining discovery. This also applies to ESI which will be used as part of the case. Figure 4.7 illustrates the procedures required for obtaining ESI.

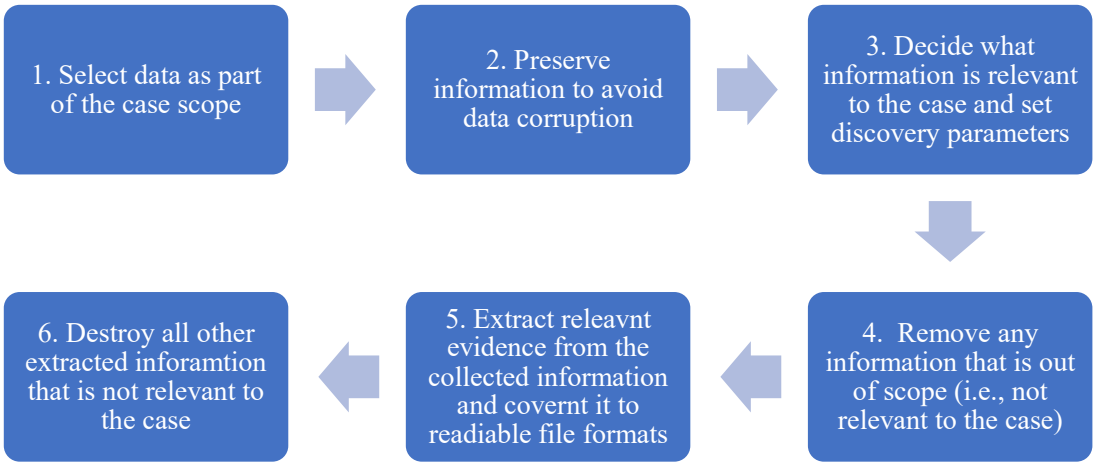


Figure 4.7: Obtaining Valid ESI Procedure

4.1.4 Phase 2 – Risk Identification

In this scenario, a quantitative risk analysis is used to calculate the risk in the next phase. Although the current scenario does not provide any historical incident data, data from a variety of sources was used to close this gap. This will help in showing how the proposed framework would be used where factual and auditable data is not available, thus reporting satisfactory risk assessment results.

4.1.4.1 Stakeholders Engagement

Beyond the team identified previously, there can unsurprisingly be stakeholders to engage, such as the opposing Legal Counsel or the CISO in a litigation matter, or employees in an internal audit. In virtually every eDiscovery matter, it can be necessary to consult the technical team on the capabilities and limitations of the eDiscovery platform. However, stakeholder engagement is built into the business process for eDiscovery (ISO, 2020b). Diverse stakeholder perceptions can lead to varying perceptions of risk, primarily influenced by differing assumptions, issues, and concerns specific to a particular risk scenario. Stakeholders often evaluate the acceptability of risk based on their understanding and perception of the risks involved (ISO, 2022a).

In general, stakeholders refer to a group of individuals who are connected to Electrooze in one way or another. They influence or may be influenced by the policies, procedures, and activities carried out by Electrooze. They are classified into two main categories: Internal Stakeholders and External Stakeholders.

Internal stakeholders are also known as the primary stakeholders of Electrooze. They are those parties, individuals, or groups that participate in the management of Electrooze and own the asset risk. Table 4.2 identifies the internal stakeholders with their responsibilities.

Table 4.2: Internal Stakeholders

Internal Stakeholder	Responsibilities
Business Owners	A group of individuals who owns an Electrooze entity (e.g., partners, shareholders).
Board of Directors	A group of individuals who governs the Electrooze entity.
Executives	A group of individuals who manage the entire unit/function/department such as the Electrooze General Manager.
Information / Asset Owners	A group of individuals who own information and make decisions. The Asset Owner has the right to access, grant permissions (e.g., read, write, and delete), and determine how the information is used.
Risk Owners	A group of individuals who collaborates to mitigate and manage the risk. Risk Owners have accountability to ensure that the treatment plan is implemented.
Employees	A group of individuals who work for Electrooze and access information.

On the other hand, external stakeholders refer to interested parties who are not a part of Electrooze management but are impacted by events that occur to Electrooze beyond their control. They are also known as the secondary stakeholders of Electrooze. Table 4.2 identifies the external stakeholders with their responsibilities.

Table 4.3: External Stakeholders

External Stakeholder	Responsibilities
Customer	A group of individuals who consumes services provided by Electrooze (e.g., in a scenario where there is a possibility of

	personal private information being inappropriately disclosed or stolen).
Court	A request to place a legal hold on data, suspend deletion policies and practices, and retain it for as long as necessary.

4.1.4.2 Assets Identification

It is important to identify what assets are at risk and then determine where value or liability exists (which will be calculated in the next activity).

In this scenario, multiple assets have been identified, including business processes, hardware, software, and information. However, the scope is limited to sensitive personal information, and it is important to acknowledge that the significance of this information is derived from the assets it intends to protect. Information discovered during the eDiscovery process is anticipated to have the most significant potential impact on the legal case. The results of the asset identification are summarised in Table 4.4.

Table 4.4: Asset Identification Results

Asset Category	Asset Identified	Asset Type	Description
Primary	eDiscovery Workflow Process	Business Processes and Activities	Preserve, collect, analyse, review, and export content that is responsive to a legal matter.
	Messages	Information	ESI extracted from emails.
	Business Files	Information	ESI extracted from business files.
	Personal Data	Information	ESI extracted from personal data.
	Databases	Information	ESI is stored on a database server.
Supporting	Web Application Server	Hardware	Provide an interface for users to access the eDiscovery platform and handles HTTPS requests.
	eDiscovery Server	Hardware	A platform that supports the legal eDiscovery process to proactively search, manage, and export ESI, including emails and other business content.
	Email Server	Hardware	Store incoming mail to be distributed among local users and handles the sending of outgoing messages.

Asset Category	Asset Identified	Asset Type	Description
	File Server	Hardware	Provide a location of shared disk access (i.e., text, image, sound, and video) that can be accessed by users.
	Database Server	Hardware	Run a database management system and provides database services to users.
	Web Application	Software	Accept requests to the eDiscovery platform via HTTPS protocol.
	eDiscovery Analyser	Software	Identify and deliver the exact collection of data required to effectively resolve a legal case.
	eDiscovery Manager	Software	Discover data that is potentially relevant to a legal matter and place that data on legal hold.
	Content Collector	Software	Archive business content into the eDiscovery platform.
	LAN	Network	Corporate connectivity.
	WAN (Internet)	Network	Cloud connectivity.
	User	Personnel	Create, process, and store information.
	Legal Counsel	Personnel	Create legal cases, search for relevant data during the discovery, and place a legal hold on the content that matches the search criteria.
	System Administrator	Personnel	Manage and maintain servers and the eDiscovery platform.
	Texas	Site	The headquarters of Electrooze.

4.1.4.3 Data Mapping

A data map is a centralised inventory that outlines the types of ESI that Electrooze possesses and where it is stored. Data mapping consists of the following elements:

- **Type of Data** – This includes a comprehensive list of all data categories, such as email, work product documents, voice mail, website content, social media content, hard copy documents, and any other types used within Electrooze.

- **Custodian** – This specifies the department, team, or personnel responsible for maintaining the data.
- **Storage Classification** – This describes the method employed for storing the data. For example, emails are stored online in an Exchange Server, nearline in an email archiving system, offline in backup tapes, and in an inaccessible format.
- **Retention Policy** – This outlines the duration for which Electrooze needs to retain the data. The retention period enables Electrooze to purge "expired" data.
- **Litigation Hold** – If the data is subject to an active litigation hold, this indicates the specific case to which the hold is applied.

Based on the identified assets previously, Table 4.5 summarises the data mapping elements.

Table 4.5: Data Mapping for Electronic Discovery

Type of Data	Custodian	Storage Classification	Retention Policy	Litigation Hold Applied
Email	System Administrator	Online	7 Years	Yes
File	System Administrator	Online	3 Years	Yes
Database	Database Administrator	Online	5 Years	No

4.1.4.4 Threats and Sources Identification

After identifying the applicable assets, now the threats associated with risk need must be identified. By analysing the nature of Electrooze and the circumstances surrounding the assets, the risk analyst can categorise the overall threat population into different communities that are relevant and applicable. It is not feasible to include every conceivable threat community in this analysis. Instead, a condensed list is generated, comprising the most likely threat communities.

Table 4.6 provides a list of possible communities that might present the sources of threats.

Table 4.6: Threat Communities List (Freund & Jones, 2014, p. 52)

Internal	External
• Employees • Contractors • Vendors • Business Partners	• Cyber criminals (professional hackers) • Organised crime • Spies • Nonprofessional hackers • Activists/hacktivist • Nation-state intelligence services • Malware/malicious code authors • Thieves

Below is a list of common threat communities for most organisations relevant to information security (Freund & Jones, 2014):

- Nation states
- Cyber criminals
- Privileged insiders
- Non-privileged insiders
- Malware

Since eDiscovery is considered a legal process involving the identification, gathering, analysis, and transfer of information (e.g., documents and email) for lawsuits, the list above can be limited to employees only, including privileged insiders and non-privileged insiders. The data obtained for eDiscovery is distinct in that it comprises precise information requested by Legal Counsel to address and resolve a legal matter. Trusted insiders may destroy, alter, or steal sensitive information. Any employee with authorised access rights poses a substantial insider threat to Electrooze if they misuse their privileges and access. Unintentional or deliberate disclosure of this information can cause various types of harm to damage Electrooze. To safeguard against unauthorised internal access and inadvertent or intentional release, a set of security measures is necessary for protecting this type of data.

In most cases, insiders often engage in actions that are either a violation of policy or unintentional. For instance, they may take sensitive information outside the workplace to work on it during non-working hours or inadvertently share sensitive information with unintended recipients. In this scenario, it is assumed that the definition of insider attacks is generally used to refer to genuinely malicious incidents (Freund & Jones, 2014).

To define a threat community, a profile is a compilation of shared characteristics linked to a specific threat community is generated. Although there is no standard set of attributes for evaluating each threat community, Table 4.7 provides common characteristics to consider for the first insider group and privileged insiders.

Table 4.7: Privileged Insider Threat Profile (Freund & Jones, 2014, p. 56)

Factor	Value
Motive	Under extreme circumstances, trusted and loyal employees may undergo a drastic change due to ruthlessness or the pursuit of personal gain.
Primary intent	Exhibit a behaviour change motivated by seeking revenge for perceived injustices or acquiring financial resources to alleviate a personal stressor.
Sponsorship	None.
Preferred General Target Characteristics	The desire for easy yet concealed financial gains or the satisfaction of targeting high-profile entities that offer a sense of validation or justification for the attackers.
Preferred Targets	Attackers tend to prefer targets they have access to.
Capability	Skillset can vary, but the attacker possesses a high-level of proficiency in the systems they have access. While they may have advanced general computer science skills, they may not necessarily excel in hacking techniques or capabilities.
Personal Risk Tolerance	The likelihood of an attacker's engagement is very low. However, certain circumstances can push them into a corner, compelling them to act. These pressures can be work-related pressure (e.g., experiencing a layoff or demotion) or personal matters (e.g., dealing with a family illness or facing financial stress).
Concern for Collateral Damage	In highly cohesive groups, there is generally a minimal tolerance for collateral damage, unless the attacker perceives mistreatment by the group.

On the other hand, non-privileged insiders are anyone who is not elevated in access privileges, including temporary workers (e.g., contractors). Electrooze must address these two groups separately due to the variance in the frequency and severity of their actions, which differ from those of privileged insiders. They differ significantly in terms of the frequency of their misconduct (i.e., engaging in a higher number of criminal activities), their skillset, and the security measures needed to address the risk they pose.

Table 4.8 provides common characteristics to consider for the second insider group, non-privileged insiders.

Table 4.8: Non-Privileged Insider Threat Profile (Freund & Jones, 2014, p. 58)

Factor	Value
Motive	Bad feeling or personal gain. These could be largely unengaged personnel with little allegiance to Electrooze organisation.
Primary intent	Gain revenge for perceived wrongs or acquire money for alleviating a personal stressor.
Sponsorship	None.
Preferred General Target Characteristics	Easy yet hidden financial gains or high-profile targets can provide vindication for the attacker.
Preferred Targets	Prefer to attack targets to which the attacker already has access, or to which they have the skills necessary to attack (i.e., in which case they would be considered privileged insiders).
Capability	Skillset varies widely. Likely to have limited access to systems. Most likely to have limited skills required for pulling off a hacking attack, yet some may be studying and practising on their own as a hobby or in pursuit of career progression.
Personal Risk Tolerance	Vary with personal circumstances.
Concern for Collateral Damage	Vary with personal circumstances.

4.1.4.5 Vulnerabilities Identification

After identifying the asset that is at risk and determining the relevant threat community, the subsequent task involves identifying the vulnerability. It should be noted that the mere existence of a vulnerability does not result in any harm, as there must be a threat present to exploit it. Vulnerabilities can be classified into various categories, such as organisational aspects, processes and procedures, management practices, personnel, physical surroundings, a configuration of information systems, hardware, software, or communications devices.

It was concluded in the previous discussion that insider attacks involve sources trusted by Electrooze to manage their data and this can be challenging to detect and prevent. Below is a list of vulnerabilities that are relevant to the insider (personnel) threat:

- Insufficient personnel presence
- Inadequate recruitment processes
- Insufficient training on security protocols
- Improper use of software and hardware
- Lack of awareness regarding security measures
- Absence of effective monitoring mechanisms
- Unsupervised activities by external or cleaning staff
- absence of policies regarding proper usage of communication methods and messaging
- Inadequate or negligent use of physical access control for buildings and rooms

From the list above, the lack of access monitoring mechanisms is considered a vulnerability candidate that corresponds to the unauthorised access threat, resulting in a risk.

4.1.4.6 Incidents and Consequences Identification

To identify the incidents and consequences in the scenario further analysis is required. Specifically, there are four types of scenarios (Group, 2013):

- **Malicious** – Refers to situations where harm is deliberately intended (e.g., an attempted theft).
- **Error** – Describes cases where an unintended action or mistake occurred (e.g., entering the wrong command at a keyboard).
- **Failure** – Pertains to instances where the action leads to unintended consequences (i.e., when the system fails to perform as intended despite the correct command given).
- **Natural** – Arises from events caused by nature (e.g., high winds).

An insider seeking to gain access to sensitive information may try any of several vectors through technical attacks, leveraging human targets, etc. Identifying the relevant vector is important because each vector may have a different frequency and different control levels. In this context, the malicious threat vector represents the possible incident and consequence scenario. Therefore, the scope scenario could be defined as "*the malicious access and misuse of sensitive information by the insiders using privileged access capabilities to the eDiscovery platform*". Subsequently, the scenario related to

Electrooze is stated as: "*Analysis of the risk associated with insiders impacting the confidentiality of the eDiscovery platform via malicious access*".

4.1.4.7 Existing Controls Identification

Electrooze has implemented an authentication control that is designed to verify the identity of a user, process, service, or device to allow access to the eDiscovery platform and other associated assets. Electrooze employed passwords and physical authenticators to authenticate identities as part of the authentication process.

4.1.5 Phase 3 – Risk Estimation

In this particular instance, qualitative terms (e.g., "High", "Medium", etc.) are assigned quantitative ranges to showcase their application to the risk analysis. This approach utilises an adapted FAIR method that incorporates a more robust quantitative analysis. This analysis is conducted using PERT distributions as inputs and employs Monte Carlo computational process for enhancing accuracy.

A set of predefined quantitative ranges will be used for the valuating asset, estimating threat, impact, and vulnerability value, and finally calculating the overall risk. It is important to note that risk analysts tend to determine the Business Impact side of the equation first. That is not a requirement. The preference here is to start with the Asset Value which works better for this adaption.

4.1.5.1 Threat Actions

Within this given scenario, Table 4.9 highlights five distinct threat actions that exhibit significant potential for causing relevant losses.

Table 4.9: Threat Actions and their Applicability

Threat Action	Applicability	Rational
Unauthorised Access	No	The insider may access sensitive information with proper authorisation. So, unauthorised access is not considered a threat action.
Misuse	No	The insider may access sensitive information with proper authorisation. So, misuse of information is not considered a threat action.
Disclosure	Yes	The insider illegally discloses information that is relevant to a litigation case. For example, the insider discloses the communication between a

Threat Action	Applicability	Rational
		lawyer and their client or third parties relating to the court proceedings, including evidence collected and tactics planned. Disclosing this information might lead to a risk of tipping their opponents off to what they are going to do. The disclosure of this information can introduce potential legal and reputation exposure.
Modification	Yes	The insider performs unauthorised changes to the information that is relevant to a litigation case. For example, the insider changes information relevant to the client or third parties relating to the court proceeding, including PII. This alternation of PII can introduce privacy impact.
Denial of Access	Yes	The insider destroys information intentionally or accidentally before a litigation case is established. For example, the insider deletes or overwrites sensitive information using a technique to make the original information non-retrievable. Data destruction can introduce productivity loss.

The identification of threat actions carried out by insiders is primarily driven by the motive of the insider (e.g., financial gain, revenge, recreation, etc.). **Given the identified threat community "The Insiders", disclosure would be the most probable threat action for the eDiscovery scenario**. Nonetheless, in certain scenarios, it might be essential to assess the loss associated with multiple threat actions separately to determine which one carries the most significant potential loss.

This analysis relies on the key assumption that the quantity of compromised sensitive information would be constrained by the number of legal cases initiated in the eDiscovery platform. Thus, it is assumed that the volume of comprised information relevant to open legal cases is relatively small.

4.1.5.2 Forms of Loss Estimation

The first step that needs to be performed is to identify which of the six loss forms is likely to materialise losses from this type of scenario as described in Table 4.10.

Table 4.10: Forms of Loss and their Applicability

Form of Loss	Loss Type	Applicable	Rational
Productivity	Primary	No	There is no operational outage, allowing Electrooze to maintain its ability to deliver services to customers without interruption. Consequently, productivity loss is not a factor to consider in this particular situation.
	Secondary	No	This is more relevant to primary loss only.
Response	Primary	Yes	The costs associated with this scenario are confined to the person-hours dedicated to the investigation and any applicable forensic activities, especially the delivery of required data in a forensically defensible manner. Consequently, response costs are considered in this particular scenario.
	Secondary	Yes	If an incident involves sensitive customer information, the consideration of response loss becomes a factor in this scenario.
Replacement	Primary	Yes	Electrooze has the authority to terminate the perpetrator directly involved in the information disclosure case, which may incur expenses related to finding a replacement unless Electrooze chooses not to fill the vacant position.
	Secondary	No	This is more relevant to primary loss only.
Fines / Judgments	Primary	No	This is more relevant to the secondary loss.
	Secondary	Yes	When handling compromises of sensitive customer information, there is always a possibility of incurring fines or judgments.
Competitive Advantage	Primary	No	This is more relevant to the secondary loss.
	Secondary	No	There is no cost involved in losing a competitive advantage. So, this type of loss is a not factor in this scenario.
Reputation	Primary	No	This is more relevant to the secondary loss.
	Secondary	Yes	Any breach of sensitive customer information carries a risk of damaging Electrooze's reputation as a possible consequence.

Among the six forms of loss mentioned in Table 4.10, the primary forms of loss typically experienced are Response and Replacement, while the other four forms of loss are considered irrelevant.

In this scenario, the primary response costs can be categorised into three categories:

- Allocation of person-hours for meetings related to the incident.
- Conducting investigations to uncover the sequence of events.
- Collaboration with law enforcement agencies.

The extent of lost costs will vary depending on the available information about the event and its accessibility. If the perpetrator confesses and it is relatively easy to determine the scope of the breach, the investigation efforts can be reduced. The presence of application logs that narrow down the number of accessed records and cross-referenced them with legitimate activities performed by the insider, can help identify the compromised information. Law enforcement agencies might also possess relevant information. However, if external forensic experts need to be brought in to ascertain the nature of the incident, the costs can quickly escalate (Freund & Jones, 2014).

The initially estimated person-hours required could range from a minimum of one hour to a maximum of 10,000 hours. Considering previous incidents of similar nature, the estimated person-hours involved in responding to this particular incident would fall within the range of 100 hours (minimum) and 200 hours (maximum). However, this estimate does not consider the number of individuals involved or the level of effort exerted. Therefore, to accommodate these factors, the estimate would be adjusted to a minimum of 50 hours and a maximum of 300 hours.

The minimum value represents a scenario with minimal complicating factors, where the insider readily admits their involvement, resulting in a limited need for investigation. On the other hand, the maximum value represents a worst-case situation where the event is more intricate, and even identifying the insider is uncertain.

As a reasonable representation of expectations, an estimate of 180 hours would be suitable for the most likely value. In this particular scenario, the selection of a high confidence level was not chosen due to numerous uncertainties surrounding the complexity of this incident.

Table 4.11 presents the primary response cost estimates after multiplying these values by Electrooze's average employee hourly rate of $35.

Table 4.11: Primary Response Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
50 hrs x $35 = $1,750	*180 hrs x $35* = $6,300	*300 hrs x $35* = $10,500	Medium

Replacement costs for a terminated employee could be estimated depending on the role that needs to be filled. The cost may involve internal recruiting costs such as recruiters' salaries and expenditures related to referral programs. External recruiting costs, on the other hand, may involve fees associated with job boards, agency services, and expenses linked to background check services. Based on the size of Electrooze, a good estimate would be a value between $5,000 (minimum) and $9,000 (maximum). Considering $7,000 would represent a reasonable most likely value. Table 4.12 presents the suggested estimates for replacement costs in this analysis.

Table 4.12: Primary Replacement Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
$5,000	$7,000	$9,000	Medium

When it comes to Secondary Loss, among the six forms of loss described in Table 4.10, Response, Fines/Judgments, and Reputation are generally the forms of loss experienced as Secondary Loss. The other three forms of loss are not relevant because they do not typically result from this type of incident.

Table 4.13 provides an estimate of the likelihood of Secondary Loss, which refers to the percentage of primary events with secondary effects that Electrooze would need to communicate with its customers regarding any breach of sensitive customer information (PII).

Table 4.13: Secondary Loss Likelihood

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
95%	98%	100%	Medium

The notification requirement is almost 100%, although there may be exceptional situations where notification is not necessary. Furthermore, two important aspects need to be considered when dealing with customer information: the customers themselves and the regulators. In the event of a sensitive customer information incident, the secondary response costs typically encompass the following:

- Costs related to customers' and regulators' notifications, if required

- Costs associated with a surge in customer support calls
- Expenditure on credit monitoring services
- Costs incurred for organising meetings to plan how to respond to customers and regulators

When the number of cases reaches a substantial level, it is highly probable that there will be costs associated with legal and public relations.

Estimating the Secondary Loss requires investigation and quantifying. Thus, some assumptions need to be made to produce reasonable estimates. The following figures will be considered as part of this estimate:

- The number of compromised records or legal cases involved in this scenario. It is estimated at 1 (minimum), 10 (most likely), and 10,000 (maximum) with moderate confidence.
- The cost of notifying customers is calculated by multiplying the estimated number of affected customers by $3 per notification.
- The estimated percentage of affected customers who may make phone calls and the average cost of each call is 10% of the total customers at $30 per call.
- The estimated percentage of customers opting for credit monitoring and the cost per customer is 10% of the total customers at $45.
- The person-hours required for meetings, taking into account the number of compromised records and legal cases, is valued at 125. To provide a range, a minimum of 50 hours, a maximum of 300 hours, and a most likely estimate of 180 hours have been considered.
- The legal cost estimation is depended on the number of compromised records. The best-case scenario assumes no legal cost ($0), while the worst-case scenario assumes all 10,000 compromised records/legal cases and estimates costs up to $100,000. The most likely estimate of $5,000 is aligned with the previously mentioned most likely number of compromised records/legal cases cited earlier (10 records/cases).
- The estimation of public relations costs is based on the number of affected customers. The best-case scenario assumes no cost ($0), while the worst-case scenario assumes all 10,000 customers are affected, and estimates costs up to $1,000,000. However, based on the expectation that a compromise of 10 records/cases would not result in any public relations

costs, the most likely cost estimate is $0.

After considering all the assumptions above, the response costs come together as presented in Table 4.14.

Table 4.14: Secondary Response Estimates

Cost	Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
Customer Notification	$3 x 1 = $3	$3 x 10 = $30	$3 x 10,000 = $30,000	Moderate
Customer Support	$0	10% x $30 x 10 = $30	10% x $30 x 10,000 =$30,000	Moderate
Credit Monitoring	$0	10% x $45 x 10 = $45	10% x $45 x 10,000 =$45,000	Moderate
Meetings	50 x $125 = $6,250	180 x $125 = $22,500	300 x $125 = $37,500	Moderate
Legal	$0	$5,000	$100,000	Moderate
Public Relations	$0	$0	$1,000,000	Moderate
Total Cost	**$6,253**	**$ 27,605**	**$ 1,242,500**	**Moderate**

The costs above are estimated using the following formulas:

- *Customer Notification Cost = Cost per Customer x # of Compromised Records/Legal Cases*
- *Customer Support Cost = % of Affected Customers x Average Cost x # of Compromised Records/Legal Cases*
- *Credit Monitoring = % of Affected Customers x Average Cost x # of Compromised Records/Legal Cases*
- *Meetings Cost = # of Hours Spent x Average Cost*
- *Legal Cost = # of Compromised Records/Legal Cases x % random*
- *Public Relations Cost = # of Compromised Records/Legal Cases x % random*

When estimating the fines/judgment loss due to legal expenses, the lowest possible amount is $0. This indicates that in the best-case scenario, where only one record or legal case is compromised, there is a genuine chance that no fines/judgments would be imposed. Even if 10 customers are affected, which is the most likely number of compromised records, it is still expected that no fines/judgments would be incurred. While there may be other associated costs they were not anticipated, resulting in a value

of $0 as well. On the other hand, the maximum estimated value presented in Table 4.15 rises to $500,000.

Table 4.15: Secondary Fine/Judgment Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
$0	$0	$500,000	Medium

Estimating the cost of reputation damage is tied to Electrooze's market share exposure. However, to determine market share exposure, two key questions need to be answered:

- What is the customer's value to Electrooze's business?
- What percentage of customers would be expected to end their service with Electrooze as a result of an incident like this?

The first question is typically quantified as the average profit generated by Electrooze from a customer throughout their relationship. In this case, the average profit per customer throughout their relationship amounts to $300. Regarding the second question, the estimation suggests a range of 10%, indicating that approximately one out of every 10 customers would choose to terminate the relationship with Electrooze. The following formula is applied to determine the reputation damage and the results are presented in Table 4.16.

Reputation Cost = The average profile per customer x # of Compromised Customer Records/Legal Cases

Table 4.16: Secondary Reputation Damage Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
$0	%5 x $300 x 10 = $150	%5 x $300 x 10,000 =$150,000	Medium

4.1.5.3 Impact Determination

To estimate the loss value, the analysis will utilise the scale provided in Table 4.17 for each form of loss that may occur in the loss event being assessed. This scale presents a range of values that help define the magnitude of the loss. The ranges within the scale depict Electrooze's capacity for losses and its tolerance levels.

Table 4.17: Loss Value Scales and Ranges

Scale	Low-End Range	High-End Range
Sever (SV)	$10,000,000	--

Scale	Low-End Range	High-End Range
High (H)	$1,000,000	$9,999,999
Significant (SG)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

Note that the reasoning provided above relies on anticipated outcomes rather than expected best and worst-case scenarios. This emphasises the inherent limitations of ordinal matrices associated with numeric ranges in accurately representing the complete range of potential results. Nevertheless, this analysis will assess the most likely value, worst-case loss, and best-case loss to reflect the infrequent occurrence of such an outcome. PERT distributions and Monte Carlo simulation techniques are used to enhance flexibility and analytical capability, especially in capturing the upper and lower ends of the possible outcomes.

The impact is determined by estimating how much money might Electrooze lose each time the loss event occurs. It is simply a combination of both Primary Loss and Secondary Loss. Based on the previous estimations, the Impact for the most likely value is calculated as follows:

Impact = Primary Loss + Secondary Loss = [Response Loss + Replacement Loss] + [Secondary Likelihood x (Response Loss + Fine/Judgement Loss + Reputation Loss)]

Impact = [$6,300 + $7,000] + [98% x ($27,605 + $0 + $150)] = $40,499.9

Thus, by using Table 4.17, the Likelihood value is set within the Significant range.

4.1.5.4 Threat Probability

People responsible for managing Electrooze business operations are considered privileged insiders. They do not pose a high level of risk, indicating that they are unlikely to engage in behaviours that result in significant losses. However, it is essential continually assess their actions. Monitoring their activities, whether as a preventive measure or to enable timely response, is crucial. Considering this, it is important to evaluate the estimates on privileged insiders.

Generally, there are two approaches to estimating the Threat Probability:

- Using historical loss data specific to this scenario, the Threat Probability can directly be estimated.

- Using a qualitative scale, such as Low, Medium, or High when there is no useful or credible data for this scenario.

When concrete data is lacking, applying a qualitative scale is often a suitable method in various situations. However, a quantitative approach offers greater clarity and is more beneficial to most decision-makers, even if it may lack precision. For instance, although risk analysts may not possess extensive empirical data on the frequency of privileged insiders disclosing sensitive information, they can make a reasonable estimation using ranges, especially if they have received adequate training in effective estimation techniques.

Based on the frequent contact between the threat community (the privileged insiders) and the information disclosed, as well as the likelihood of them taking action against such information, an estimate of Threat Probability can be made.

Considering that privileged insiders are generally composed of trustworthy individuals, who typically do not place significant and valuable on sensitive information and may perceive high risks associated with illegal usage, it appears reasonable to estimate a Low Threat Probability using Table 4.18.

Table 4.18: Threat Probability Ranges

Scale	Ranges
Very High (VH)	> 50 times per year
High (H)	Between 20 and 50 times per year
Moderate (M)	Between 1 and 20 times per year
Low (L)	Between 0.1 and 2 times per year
Very Low (VL)	<0.1 times per year (less than once every 20 years)

A privileged insider may possess motive and sufficient computing experience to recognise and exploit the potential value of sensitive information. Furthermore, they may have a high enough risk tolerance to engage in illegal activities. However, considering the various factors involved, the frequency of such incidents is expected to be relatively low.

Alternatively, if there is historical data available, it becomes possible to estimate the Threat Probability. In certain cases, it is conceivable that out of a population of 30 individuals with no criminal records, there would be one or more individuals engaging in over 50 malicious acts per year. Table 4.19 presents the estimates of the Threat Probability, which is a common occurrence when limited historical information is available regarding privileged insider incidents.

Table 4.19: Threat Probability Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
0.05 (once every 20 years)	0.1 time per year (twice every 20 years)	50 times per year	Medium

4.1.5.5 Vulnerability Probability

Vulnerability refers to the likelihood of a threat event transitioning to a loss event. The vulnerability arises when there is a disparity between the force being exerted by the threat agent, and the object's ability to withstand that force. Determining the Vulnerability requires two primary factors: Threat Capability and Control Strength.

4.1.5.6 Threat Capability Estimation

Threat Capability pertains to the skill (knowledge and experience) and resources (time and materials) possessed by privileged insiders that enable them to successfully disclose information against the eDiscovery platform. In this context, the primary objective is to estimate the average privileged insider's proficiency in finding sensitive information and the time they can allocate to this task. Assessing the Threat Capability is a challenging aspect of the analysis. However, it is justifiable to assign a Modetate to the Threat Capability of the privileged insiders, indicating average skill and resources when compared to the overall threat population. The estimation of Threat Capability is always related to the specific scenario.

Table 4.20 presents a percentile scale ranging from 2 to 98, which encompasses the complete range of capabilities exhibited by a population of threat agents (referred to as the Threat Capability Continuum). With this continuum, the least capable privileged insider in the population is associated with the 2nd percentile, whereas the most capable privileged insider represents the 98th percentile. The remaining individuals within the population fall at various points between these extremes.

Table 4.20: Threat Capability Ranges

Scale	Ranges
Very High (VH)	Top 2% when compared against the overall threat population (98th percentile)
High (H)	Top 16% when compared against the overall threat population (between the 84th and 98th percentiles)
Moderate (M)	Average skill and resources, between the bottom 16% and top 16% (between the 16th and 84th percentiles)

Scale	Ranges
Low (L)	Bottom 16% when compared against the overall threat population (below the 16th percentile)
Very Low (VL)	Bottom 2% when compared against the overall threat population (below the 2nd percentile)

In this scenario, the least skilled privileged insider resides at the bottom 2%, while the most skilled individual falls within the top 98%. The highest level of privileged insider is held by someone around the 84th percentile. This estimation is based on the assumption that the privileged insider possesses limited expertise and resources.

4.1.5.7 Control Strength Estimation

Control Strength refers to the anticipated level of effectiveness of security measures within a specified timeframe, compared to a standard level of force or the asset's inherent resistance to compromise. Essentially, it assesses the robustness of controls and protective mechanisms designed to thwart potential attacks.

The Threat Capability Continuum serves as a scale to gauge the impact of controls on the level of difficulty faced by threat agents attempting to overcome them. To be considered meaningful, control should either increase the difficulty for threat agents in malicious or natural disaster scenarios or reduce the difficulty in scenarios involving human error.

In this scenario, Eletrooze has implemented authentication control which is commonly relevant in a malicious scenario. Authentication control is an avoidance/preventive control that minimises the occurrence of information disclosure events and decreases the probability of occurrence.

To assess the effectiveness of the authentication control, an estimation can be made that individuals below the 70th percentile of the Threat Capability Continuum would be prevented by bypassing the control. Conversely, it is estimated that individuals above the 90th percentile are highly likely to succeed in overcoming the control. These estimates represent the extremes of the distribution.

The most likely value for the authentication control's effectiveness is estimated to be around the 84th percentile as indicated in Table 4.21. This implies that Electrooze is reasonably well-protected against an average threat population because the authentication control exhibits a Moderate level of effectiveness. It is important to note that the Difficulty level is always evaluated in relation to the Threat Capability Continuum, which

serves as a measurement scale and pertains to the specific threat community analysed in this scenario.

Table 4.21: Control Strength Ranges

Scale	Ranges
Very High (VH)	Protects against all but the top 2% of an average threat population (98th percentile)
High (H)	Protects against all but the top 16% of an average threat population (between the 84th and 98th percentiles)
Moderate (M)	Protects against the average threat agent (between the 16th and 84th percentiles)
Low (L)	Only protects against the bottom 16% of an average threat population (below the 16th percentile)
Very Low (VL)	Only protects against the bottom 2% of an average threat population (below the 2nd percentile)

4.1.5.8 Vulnerability Determination

Vulnerability can be estimated directly without estimating Threat Capability and Control Strength. This case is a privileged insider scenario, and Electrooze is 100% vulnerable to a threat event. However, the aim here is to show how vulnerability can be derived using Figure 4.8.

Determining the Vulnerability can be achieved by finding the Threat Capability on the vertical axis side of the matrix and the Control Strength on the horizontal axis. The point of intersection between these two factors indicates Vulnerability. For this scenario, as illustrated in Figure 4.8 (a dashed box), a Moderate Threat Capability combined with a Moderate Control Strength results in a Moderate Vulnerability.

Threat Capability	Very Low	Low	Moderate	High	Very High
Very High	Very High	Very High	Very High	High	Moderate
High	Very High	Very High	High	Moderate	Low
Moderate	Very High	High	Moderate	Low	Very Low
Low	High	Moderate	Low	Very Low	Very Low
Very Low	Moderate	Low	Very Low	Very Low	Very Low

Control Strength

Figure 4.8: Vulnerability Matrix

4.1.5.9 Likelihood Determination

In this scenario, when considering a Low Threat Probability and a Moderate Vulnerability, the Likelihood is determined to be Low as illustrated in Figure 4.9. Since

Vulnerability is expressed as a percentage, it can never exceed 100%. Therefore, the Likelihood will never surpass the Threat Probability.

Threat Probability	Very Low	Low	Moderate	High	Very High
Very High	Moderate	High	Very High	Very High	Very High
High	Low	Moderate	High	High	High
Moderate	Very Low	Low	Moderate	Moderate	Moderate
Low	Very Low	Very Low	Low	Low	Low
Very Low	Very Low	Very Low	Very Low	Very Low	Very Low

Vulnerability

Figure 4.9: Likelihood Matrix

4.1.5.10 Risk Level Determination

To determine the Risk Level for this scenario, the Impact score (i.e., this is static and does not vary between scenarios) is compared to the Likelihood. Given an Impact of Significant and a Likelihood of Low, the Risk Level would be Moderate as shown in Figure 4.10.

Impact	Very Low	Low	Moderate	High	Very High
Very High	High	High	Critical	Critical	Critical
High	Moderate	High	High	Critical	Critical
Significant	Moderate	Moderate	High	High	Critical
Moderate	Low	Moderate	Moderate	High	High
Low	Low	Low	Moderate	Moderate	Moderate
Very Low	Low	Low	Moderate	Moderate	Moderate

Likelihood

Figure 4.10: Risk Level Matrix

In this analysis, it is possible to evaluate multiple threat communities or various types of loss events. However, focusing on evaluating the most likely and significant scenario can often provide sufficient information for decision-makers to determine the cost-effective risk mitigation for Electrooze.

4.1.6 Phase 4 – Risk Evaluation and Treatment

After acquiring the estimates, the results of the analysis above can be computed. After gathering all the relevant estimates, the data was entered into the FAIR-U tool as presented in Table 4.22.

Table 4.22: Risk Components for Insider Malicious Access

Scenario 1 - Collecting Electronic Content for Legal Cases

Purpose	Asset	Threat Community	Threat Type	Threat Effect
Analysis of the risk associated with insiders impacting the confidentiality of the eDiscovery platform via malicious access	eDiscovery Platform	Insiders	Malicious	Confidentiality

Primary Loss	Min	ML	Max	Confidence
Productivity	$0	$0	$0	Medium
Response	$1,750	$6,300	$10,500	Medium
Replacement	$5,000	$7,000	$9,000	Medium
Competitive Advantage	$0	$0	$0	Medium
Fines and Judgments	$0	$0	$0	Medium
Reputation	$0	$0	$0	Medium

Secondary Loss	Min	ML	Max	Confidence
Productivity	$0	$0	$0	Medium
Response	$6,253	$27,605	$1,242,500	Medium
Replacement	$0	$0	$0	Medium
Competitive Advantage	$0	$0	$0	Medium
Fines and Judgments	$0	$0	$500,000	Medium
Reputation	$0	$150	$150,000	Medium

	Min	ML	Max	Confidence
Likelihood (Frequency of Events)	0.05	0.1	50	Medium
Secondary Likelihood	95%	98%	100%	Medium
Threat Capability	2%	84%	98%	Medium
Control Strength	70%	84%	90%	Medium

The tool executes 50,000 Monte Carlo simulations to estimate the probable range of ALE in dollars as a loss exceedance curve. The screenshots in both Figure 4.11 and Figure 4.12 show the simulation output of the analysis above. They present the ALE derived from the estimated probable frequency (Likelihood) and projected probable future losses (Impact) for this scenario.

Figure 4.11: Annualised Loss Exposure with Linear Scale for Scenario 1

The 10th and 90th percentiles show where 80% of the simulated results fell. The Most Likely amount shows the ALE that occurred most frequently in the simulated results. The $930,400 Most Likely figure represents that in most simulated years, the Loss Event would not occur.

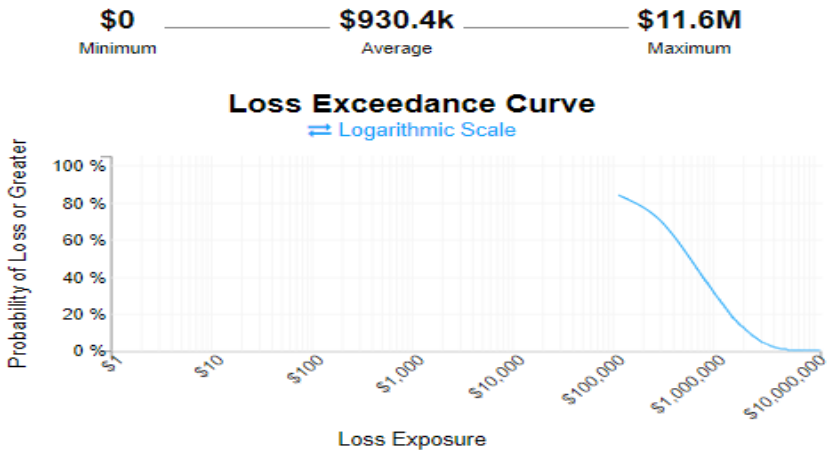


Figure 4.12: Annualised Loss Exposure with Logarithmic Scale for Scenario 1

Table 4.23 details the results of the simulation based on the estimated variable inputs. It shows the projected number of Primary Loss events per year and their corresponding associated losses. Additionally, it presents the forecasted number of Secondary Loss events per year along with associated losses. Finally, the FAIR-U tool provides the calculated ALE results.

Table 4.23: Summary of Simulation Results for Scenario 1

Primary

	Min	Avg.	Max
Likelihood (Loss Events / Year)	0	2.67	15
Impact (Loss Value)	$7.6k	$13.2k	$18.6k

Secondary

	Min	Avg.	Max
Likelihood (Loss Events / Year)	0	2.66	15
Impact (Loss Value)	$13.2k	$335.0k	$1.3M

Vulnerability 32.29%

The next section will focus on analysing the outcomes above to communicate them to the relevant stakeholders.

4.1.6.1 Risk Acceptance Options

Reviewing the results above help Electrooze in understanding the current risk and the decisions that need to be made (either accept, avoid, transfer, or treat). The first thing that should be looked at is the most likelihood of ALE. The $930,400 seems to be a reasonable value from a credibility perspective.

As mentioned earlier, it has been emphasised that qualitative expressions of Risk Level (e.g., High, Moderate, etc.) should align with Electrooze's loss capacity and subjective risk tolerance. For instance, the scale can be understood to indicate that an impact exceeding $1M would be categorised as a High risk and typically treated as such by monitoring users' activities or implementing an encryption solution at the data layer to mitigate the potential exposure.

Another important aspect here is to look at the maximum value of ALE, which is roughly $12M. However, an important observation can be made about this value within the context of this scenario. It is largely influenced by the maximum number of Primary Loss events, which is 15. This implies that for Electrooze to incur this level of loss, it would have to encounter all 15 of these loss events. In other words, after the first event, Electrooze would need to make any required changes to prevent the other 14 from happening. This is true, assuming that Electrooze is aware of the first event that took place. However, it is plausible for these events to take place unnoticed for an extended period, potentially enabling a privileged insider to carry out 15 malicious activities before anyone detects them. In such a case, Electrooze would incur financial losses to cover these damages.

4.1.6.2 Risk Treatment Plan

After discussing the current risk, the next step is to focus on potential control measures. The apparent issue is the need to enhance authentication control, as its current implementation is not producing the expected results when implemented in isolation. This could be achieved by adding multi-factor authentication (e.g., a combination of passwords and PIN, token ID, or biometric) capability to the existing authentication mechanism (for accessing both privileged and non-privileged accounts).

Assuming the possibility that a population of 15 individuals with no criminal records, there exists the potential for one or more individuals to engage in 25 malicious acts per year, as presented in Table 4.24.

Table 4.24: Threat Probability Estimates (After Halving Variables)

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
0.025 (once every 40 years)	0.05 times per year (twice every 40 years)	25 times per year	Medium

By enhancing the mentioned control to limit authorised access for insiders by half, the maximum ALE would also be reduced by half (5M), as shown in Figure 4.14. The expenses associated with improving the authentication process are relatively small, yet the potential return on investment can result in a substantial reduction of risks.

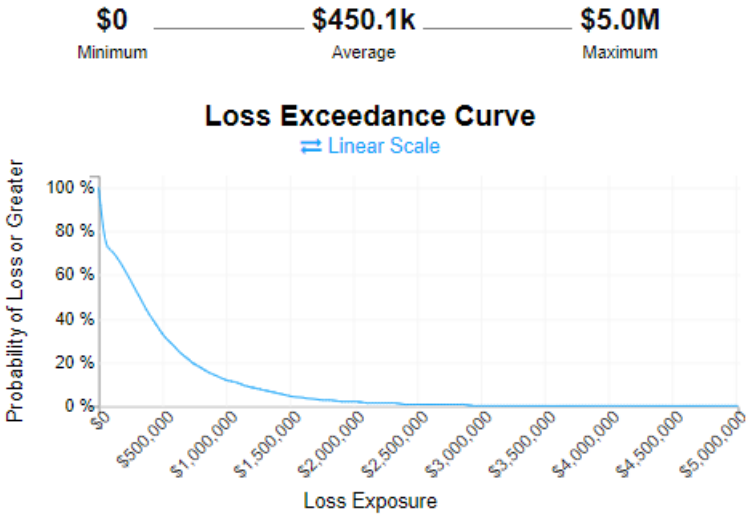


Figure 4.13: Annualised Loss Exposure after Halving Threat Probability Variables

Another control opportunity arises from restricting the number of customer accounts each user can access. This can be facilitated if Electrooze implements a logical

distribution of responsibilities, such as by geographic region or other criteria. Similarly, after considering a halving of customer numbers, the secondary response costs align accordingly, as presented in Table 4.25.

Table 4.25: Secondary Response Estimates (After Halving Number of Customers)

Cost	Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
Customer Notification	$3 x 0.5 = $1.5	$3 x 5 = $15	$3 x 5,000 = $15,000	Medium
Customer Support	$0	10% x $30 x 5 = $15	10% x $30 x 5,000 =$15,000	Medium
Credit Monitoring	$0	10% x $45 x 5 = $22.5	10% x $45 x 5,000 =$22,500	Medium
Meetings	50 x $125 = $6,250	180 x $125 = $22,500	300 x $125 = $37,500	Medium
Legal	$0	$2,500	$50,000	Medium
Public Relations	$0	$0	$500,000	Medium
Total Cost	**$6,251.5**	**$ 25,052.5**	**$ 595,000**	**Medium**

If this change was applied, wherein instead of all 10,000 customers having access to the range, such as 5,000, the loss value estimates would be lower. Consequently, this adjustment would significantly impact both the maximum and average level of risks, as illustrated in Figure 4.14, where the ALE is $6.4M

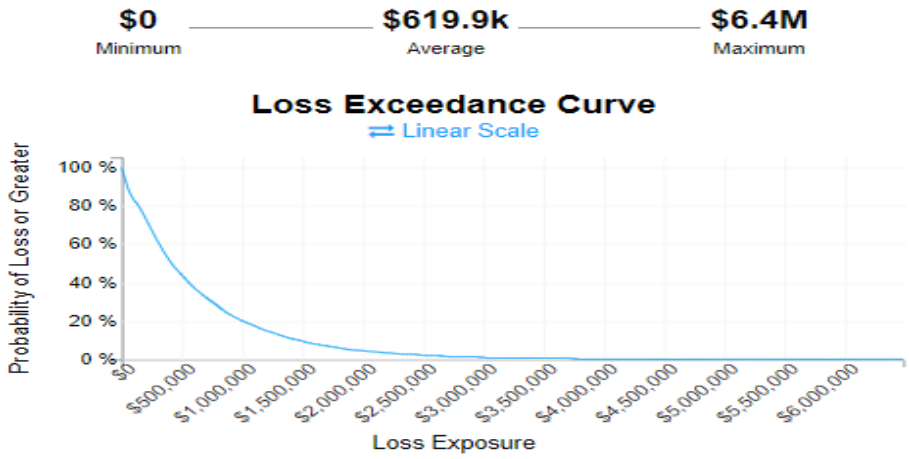


Figure 4.14: Annualised Loss Exposure after Adding Number of Customers for Scenario 1

It is important to note here that such a change would not only impact the risk associated with this particular scenario but also extend to every other scenario involving

malicious activities against the eDiscovery platform. Consequently, it would contribute to reducing risk across various contexts.

Another opportunity for control implementation is through the use of logging control. By establishing normal values for the number of customer records accessed by each user, the eDiscovery platform's logging system could identify instances where user access deviates significantly from the norm. This would serve as an early warning mechanism, alerting to suspicious activity. For example, if a user accessed 50 records in a day when the normal value was 20, it would suggest potential wrongdoing. Similarly, if a user's normal activity was 20 and suddenly dropped to 0, it could indicate that the access still exists, but the user is inactive, possibly due to a failure in the authentication management process or the user being on vacation. In such cases, it would be prudent to set up a warning system if the prolonged drop-off persists for a specific period.

To add another control is to implement an encryption solution at the data layer (i.e., encryption at rest). Encryption is an avoidance/preventive control that keeps the occurrence of information disclosure events. In other words, encryption control decreases the probability of contact. When considering the compromise of sensitive information, encrypted information demonstrates a strong level of control (i.e., likely at the top 2%) compared to unencrypted information.

Encryption at rest is designed to safeguard against unauthorised disclosure and alteration of sensitive information stored in various storage infrastructures such as emails, files, and databases. It is a key protection against data breaches and specifically pertains to the state of information when it is not actively being processed or transmitted but rather resides on system components like an eDiscovery platform.

In order to assess the efficacy of the encryption control, it is projected that the control will prevent individuals below the 90^{th} percentile along with the Threat Capability Continuum from succeeding. Conversely, those above the 98^{th} percentile are expected to have a guaranteed success rate, representing the two extremes of this distribution. The estimated value at the 95^{th} percentile is considered the most likely, indicating a High level of effectiveness for the encryption control (see Table 4.21 for reference).

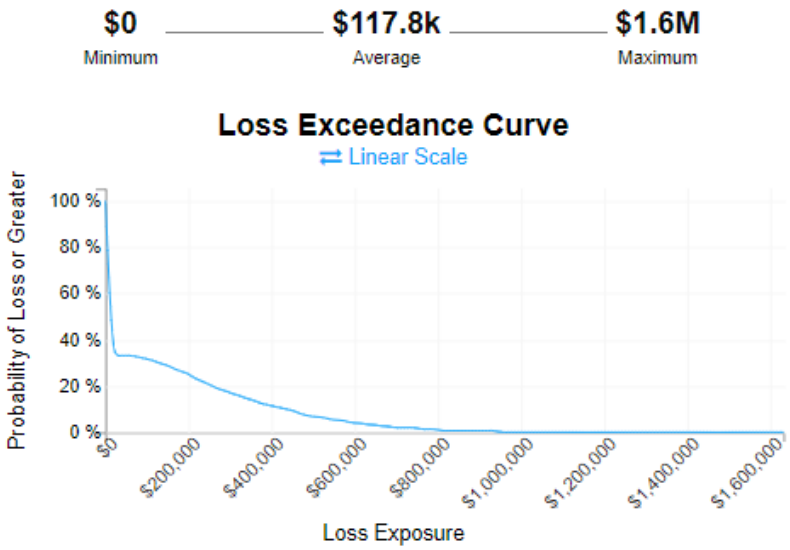


Figure 4.15: Annualised Loss Exposure after Implementing Encryption Control for Scenario 1

Figure 4.15 suggests that there will be a big drop in terms of the ALE maximum value (from 11M to 1.6M) if the encryption control is implemented. Hence, introducing encryption control into the Electrooze environment would improve the overall security measures and decrease the risk to a level that is considered acceptable. The rationale behind that is that encryption has a strong resistance capability in preventing any attempt to disclose sensitive information in an unauthorised manner.

4.1.6.3 Risk Prioritisation

The final step in this activity is to determine which risk Electrooze should act upon first. The prioritisation and implementation timeframe of individual risk treatments should be determined based on the Likelihood and Impact during the risk estimation process. The previously discussed risk treatment plan should outline this order of priority for executing the necessary risk mitigation measures.

Different approaches, including risk ranking and cost-benefit analysis, can be employed to establish priorities. In this scenario, Electrooze is tasked with determining the appropriate balance between the costs associated with implementing additional controls and the allocation of the budget. Various controls were proposed including improving the authentication process, limiting the number of users accessing the eDiscovery platform, considering the users' activity logging option, and implementing an encryption solution to reduce the overall risk with a minimum value of the ALE.

4.1.7 Phase 5 – Monitoring and Improvement

When Electrooze decided to implement additional controls to minimise the overall risk, the identified risks and their relevant components (i.e., asset valuation, impact, events, threat community, threat probability, forms of loss, vulnerability, and control strength) should be monitored and reviewed.

By doing so, Eletrooze would be able to promptly identify any necessary changes and maintain a better understanding of the entire scope of risk. Consequently, the risk management process would be improved by consistently aligning the management of risks with Electrooze's business objectives and considering the available risk acceptance options.

4.1.8 Errors and Omission

In this scenario, the Threat Community was a privileged insider and the Vulnerability was derived from estimates of Threat Capability and Control Strength. This approach has a problem because, for any scenario involving privileged insiders, Electrooze must be 100% vulnerable. Therefore, the Vulnerability must be directly estimated without deriving it from the Threat Capability and Control Strength.

It is important to not go any deeper in the analysis. The risk analysts should initiate their assessment from the highest level of the FAIR ontology, specifically for the Likelihood aspect. They should consider whether it is feasible to directly estimate the Likelihood rather than attempting to estimate Threat Probability and Vulnerability to derive it. During the scenario testing, the researcher found that the Assets Valuation activity did not fit with the FAIR model ontology as part of the Risk Identification process as illustrated in Figure 4.16.

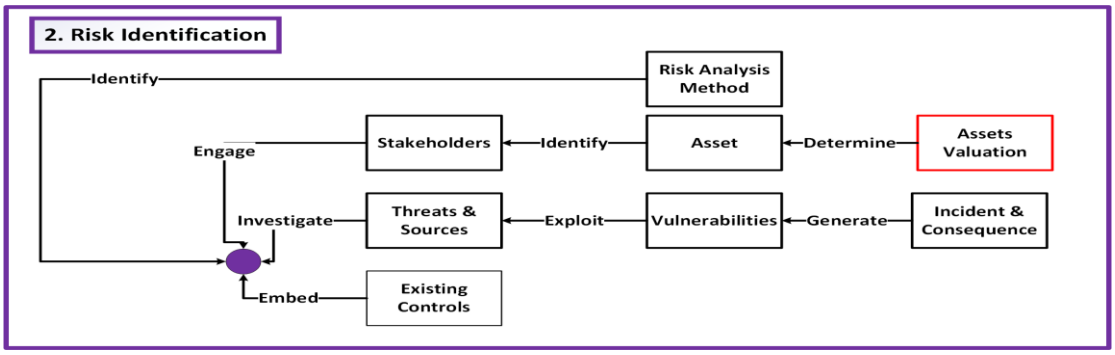


Figure 4.16: Assets Valuation component as part of the Risk Identification process

Instead, data mapping should be introduced as an appropriate activity that has a centralised inventory outlining the types of ESI an organisation possesses and their

locations as illustrated in Figure 4.17. Data mapping is a more structured and cohesive approach to identifying threats and sources. It also helps risk analysts create a DFD and BPM based on various risk scenarios. Moreover, data mapping focuses on sensitive personal information, recognising that its significance is derived from its intended purpose of safeguarding such information, especially in relation to the eDiscovery process.

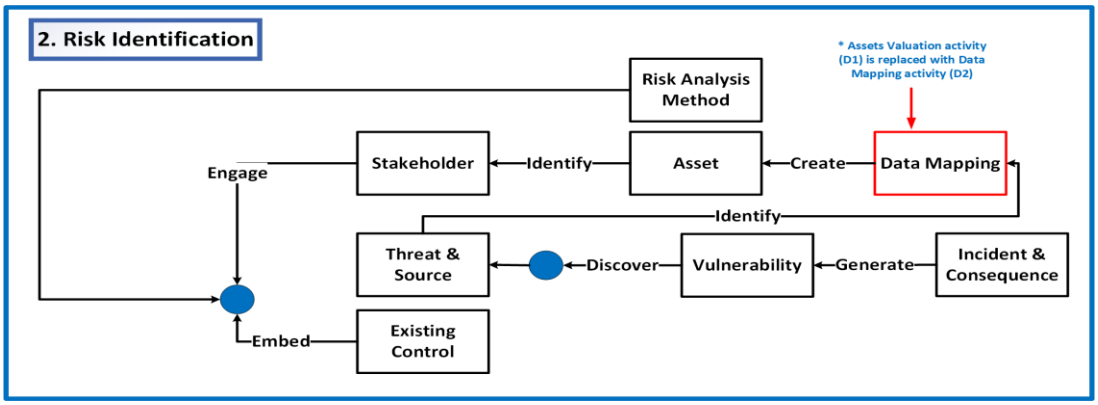


Figure 4.17: Introducing a New Component into Risk Identification Process

4.2 SCENARIO 2 – PROTECTING THIRD-PARTIES INTELLECTUAL PROPERTY (IP) FROM DATA LEAKAGE

This scenario explains the data leakage issue that organisations face when they store the IP of third parties in multiple locations. There are many issues that organisations face while moving their data and systems to the cloud. Using a SaaS-based eDiscovery solution introduces risks from two key perspectives: data residing in the cloud (i.e., data sovereignty) and discovery technology implemented in the cloud. On the other hand, when data is split between on-premises and cloud environments, transferring data between them introduces more security risks.

4.2.1 Define Scenario

Trendooze is a SaaS provider partnering with businesses to help them create bespoke marketing plans. Trendooze was established in 2015 and has a single office located in Sydney, Australia serving hundreds of customers. Trendooze has more than 70 vendors and partners across the Asia-Pacific region. Due to the current COVID-19 pandemic, Trendooze announced a new policy that allows 600 employees to work from home (WFH) for more agility and flexibility in working arrangements.

Over the past three years, Trendooze has undergone substantial growth due to the arrival of startup organisations that subscribed to Trendooze's services.

There are hundreds of millions of sensitive third-party IP files such as technical drawings and structured data. Those files are scattered across various systems and hosted in distinct geographical locations (e.g., on-premises and public clouds) as illustrated in Figure 4.18. Trendooze faces challenges to use all available means to define instances of commercially sensitive third-party IP and apply a data removal solution to remediate this risk. The definitions for what was considered in the scope and applying a removal process from the third-party's systems were constantly evolving. The scale of documents identified for review and remediation is significantly larger than that typically seen in a major litigation or investigation case.

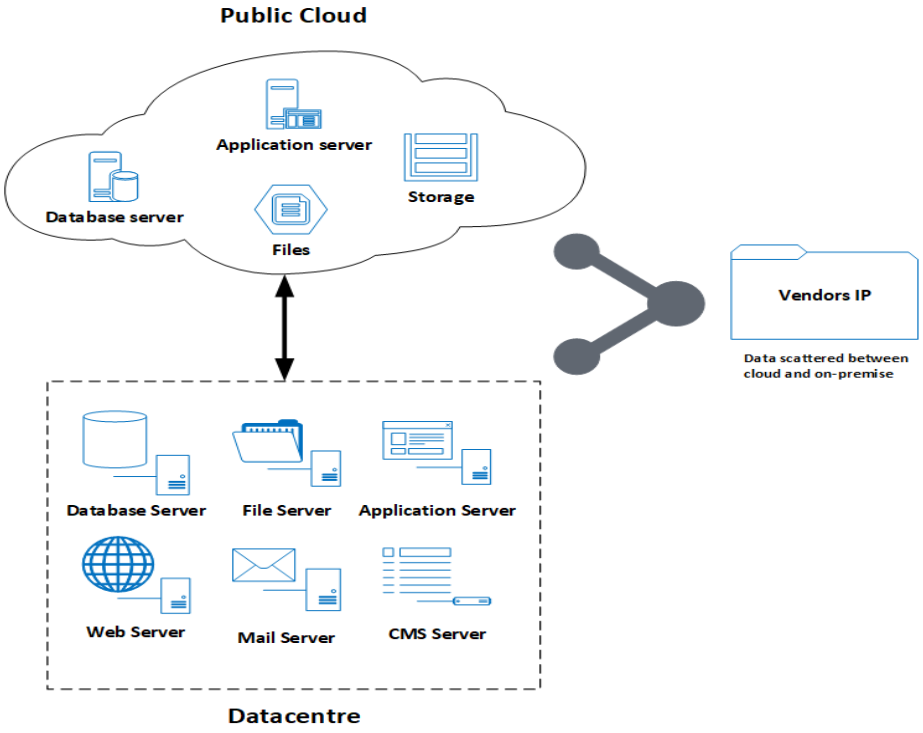


Figure 4.18: Third-Parties IP Transferred between Cloud and On-Premises Network

4.2.2 Test Artefact 1 Framework

This scenario is tested using the first artefact of the proposed framework. This section explains how the proposed framework is tested.

To determine Trendooze's top risks, the CISO updated their Risk Register. The CISO found that IP leakage is a top risk to Trendooze. Phishing campaigns are one of the top vectors by which threat actors gain a foothold into the Trendooze network and possibly steal sensitive data.

A thorough analysis has revealed that the most risk exposure for Trendooze lies in the potential breach of the eCommerce database, which is supported by several critical systems relied upon by Trendooze. It is an internal database that stores third-party information, including company brands, marketing strategies, patents, and trademarks. As part of Trendooz's assurance program, the CISO requested the Risk Team to conduct a full risk analysis. While Trendooze is not a target for nation-state actors, Trendooze is occasionally targeted by groups of cyber criminals.

The scope scenario is defined as "*the malicious access and misuse of sensitive information by cyber criminals using phishing campaigns capabilities to the eCommerce database*". Subsequently, the scenario related to Trendooze is: "*Analysis of the risk associated with cyber criminals impacting the confidentiality of third-party IP in the eCommerce database via a phishing attack*".

Trendooze has implemented an Email filtering solution that catches around 80% of phishing emails. On the other hand, there are only around 20% of convincing phishing emails are opened. Since the identified threat community is cyber criminals, disclosure would be the most probable threat action for the eCommerce database scenario. Table 4.26 presents the applicability of the six likely loss forms that will materialise losses from this type of scenario.

Table 4.26: Forms of Loss and Their Applicability

Form of Loss	Loss Type	Applicable
Productivity	Primary	No
	Secondary	No
Response	Primary	Yes
	Secondary	Yes
Replacement	Primary	No
	Secondary	No
Fines / Judgments	Primary	No
	Secondary	Yes
Competitive Advantage	Primary	No
	Secondary	No
Reputation	Primary	No
	Secondary	Yes

Among the six forms of loss detailed in Table 4.26, the forms commonly experienced by Trendooze include Primary and Secondary Responses, Secondary Fines /

Judgments, and Reputation. The remaining four forms of loss are not applicable in this context.

In the event of a security breach, Trendooze has a dedicated team of 10-15 incident response analysts who require 8-24 hours to respond to an incident with an average employee hourly rate of $60. In addition to that, Trendooze would engage an external forensic team to investigate the extent of the data breach and the methods employed by the perpetrators. Typically, investigations of this magnitude incur an average cost of $90,000. Subsequently, the primary response cost estimates are presented in Table 4.27.

Table 4.27: Primary Response Estimates

Incident Response	Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
Internal Incident Response	*10 people x 8 hours x $60/hr = $4,800*	*12 people x 16 hours x $60/hr =$11,520*	*15 people x 24 hours x $60/hr =$21,600*	*Medium*
External Incident Response	*$60,000*	*$90,000*	*$120,000*	*Medium*
Total	*$64,800*	*$101,520*	*$141,600*	*Medium*

When dealing with sensitive third-party information scenarios, Trendooze would always have to engage third parties if their IP has been breached. Hence, the likelihood of Secondary Loss, which refers to the percentage of primary events leading to secondary effects, can be found in Table 4.28.

Table 4.28: Secondary Loss Likelihood

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
95%	98%	100%	Medium

The assumptions below are required to estimate the secondary response loss:

- Approximately 5,000 third parties use the eCommerce platform on an annual basis, and only 1,500 third parties have stored their IP on the eCommerce platform.
- Notifying impacted third parties will cost around $20 per third party.
- Trendooze has a contract in place to provide platform monitoring to third parties impacted by a breach. The cost is $30-35 per third party.

After considering all the assumptions above, the costs associated with the secondary response are estimated in Table 4.29.

Table 4.29: Secondary Response Estimates

Item	Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
Third-Party Notification	1,500 x $20 = $30,000	1,500 x $20 = $30,000	1,500 x $20 = $30,000	Moderate
eCommerce Platform Monitoring	1,500 x $30 = $45,000	1,500 x $33 = $49,500	1,500 x $35 = $52,500	Moderate
Total Cost	**$75,000**	**$79,500**	**$82,500**	**Moderate**

In the last three years, fines imposed for breaches involving the intellectual property of more than 1,500 third parties IP have varied between $150,000 and $500,000. Then, the secondary fine/judgment is estimated in Table 4.30.

Table 4.30: Secondary Fine/Judgment Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
$150,000	$350,000	$500,000	Medium

The eCommerce platform generates an annual revenue of approximately $8.5 million, and on average, the value of each third-party is estimated to be around $200. In the event of a security breach, it is estimated that 3% of affected third parties would stop subscribing to Trendooze services and choose a competitor going forward. This means approximately 45 third parties would no longer do business with Trendooze, and the average value of a customer is $3,000. Table 4.31 presents the estimated cost of the security reputation damage.

Table 4.31: Secondary Reputation Damage Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
1,500 x 3% x $2,000 = $90,000	1,500 x 3% x $2,500 =$112,500	1,500 x 3% x $3,000 =$135,000	Medium

The impact is calculated by combining both Primary Loss and Secondary Loss. Based on the previous estimations, the Impact (for most likely value) will be as follows:

Impact = Primacy Response Loss + [Secondary Likelihood x (Secondary Response Loss + Secondary Fine/Judgement Loss + Secondary Reputation Loss)]

Impact = $101,520 + [98% x ($79,500 + $350,000 + $112,500)] = $530,670

Thus, by using Table 4.17, the Impact value is set within the Significant range. Also recognising cyber criminal activity levels, it is estimated as a Moderate Threat Probability using Table 4.32.

Table 4.32: Threat Probability Ranges

Scale	Ranges
Very High (VH)	> 12 times per year (more than once every month)
High (H)	Between 6 and 12 times per year
Moderate (M)	Between 2 and 6 times per year
Low (L)	Between 0.1 and 2 times per year
Very Low (VL)	<0.1 times per year (less than once every 2 years)

Table 4.33 provides the estimates of the Threat Probability. This is a common occurrence in cyber-criminal activities, particularly when there is limited historical data available to analyse.

Table 4.33: Threat Probability Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
0.05 (once in 2 years)	2 (twice a year)	12 (once a month)	Medium

Using Table 4.20, the threat capability is estimated as follows. The most capable cybercriminal sets within a Very High scale. The rationale for this estimate is that a cybercriminal is more skilled and has the resources to craft phishing attacks.

It has been identified previously that Trendooze has implemented an Email filtering solution that blocks 80% of incoming phishing emails. Table 4.21 is a baseline to estimate the Control Strength, and then the Moderate scale is the best fit (80% sets between the 16^{th} and 84^{th} percentiles). Then, if the risk analyst combines both Very High Threat Capability with a Moderate Control Strength, the Vulnerability result is Very High based on Figure 4.8.

In this particular scenario, considering a Moderate Threat Probability and a Very High Vulnerability, the Likelihood would be Moderate based on Figure 4.9. The Impact score is compared to the Likelihood that is determined. Given an Impact of Significant and a Likelihood of Moderate, the Risk Level would be High based on Figure 4.10.

Once the relevant numbers have been obtained, it is time to use them and observe the outcomes of the analysis. Table 4.34 presents the estimates entered in the FAIR tool.

Table 4.34: Risk Components for Cyber Criminals Fishing Attacks

Scenario 2 - Collecting Electronic Content for Legal Cases

Purpose	Asset	Threat Community	Threat Type	Threat Effect
Analysis of the risk associated with cyber criminals impacting the confidentiality of third-party IP in the eCommerce database via a phishing attack	eCommerce Platform	Cyber Criminals	Malicious	Confidentiality

Primary Loss	Min	ML	Max	Confidence
Productivity	$0	$0	$0	Medium
Response	$64,800	$101,520	$141,600	Medium
Replacement	$0	$0	$0	Medium
Competitive Advantage	$0	$0	$0	Medium
Fines and Judgments	$0	$0	$0	Medium
Reputation	$0	$0	$0	Medium

Secondary Loss	Min	ML	Max	Confidence
Productivity	$0	$0	$0	Medium
Response	$75,000	$79,500	$82,500	Medium
Replacement	$0	$0	$0	Medium
Competitive Advantage	$0	$0	$0	Medium
Fines and Judgments	$150,000	$350,000	$500,000	Medium
Reputation	$90,000	$112,500	$135,000	Medium

	Min	ML	Max	Confidence
Likelihood (Frequency of Events)	0.05	2	12	Medium
Secondary Likelihood	95%	98%	100%	Medium
Threat Capability	2%	84%	98%	Medium
Control Strength	65%	80%	90%	Medium

The screenshots in Figure 4.19 and Figure 4.20 illustrate the simulation output of the analysis above. These screenshots present the ALE derived from the estimated Likelihood and Impact of probable future losses for this specific scenario.

Figure 4.19: Annualised Loss Exposure with Linear Scale for Scenario 2

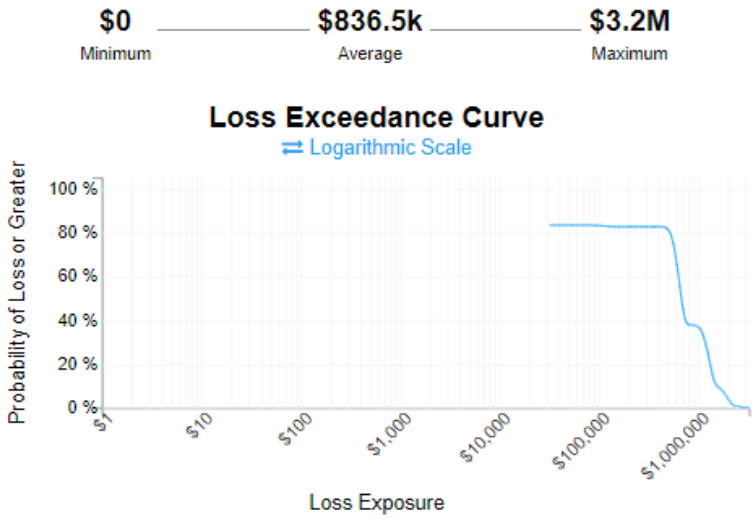


Figure 4.20: Annualised Loss Exposure with Logarithmic Scale for Scenario 2

Table 4.35 details the results of the simulation based on the estimated variable inputs. It shows the projected number of primary loss events anticipated annually, along with the associated loss amount for each event. It also shows the estimated number of Secondary Loss events expected per year, the corresponding loss amount, and the resulting ALE outcomes.

Table 4.35: Summary of Simulation Results for Scenario 2

Primary

	Min	Avg.	Max
Likelihood (Loss Events / Year)	0	1.34	5
Impact (Loss Value)	$66.1k	$102.2k	$140.3k

Secondary

	Min	Avg.	Max
Likelihood (Loss Events / Year)	0	1.31	5
Impact (Loss Value)	$350.9k	$533.1k	$698.6k

Vulnerability 39.94%

The $836,500 is a reasonable value from a credibility perspective. An interpretation of this amount suggests that any impact exceeding $900,000 will be categorised as a High risk and typically addressed accordingly by implementing additional controls to mitigate the exposure.

It is important to focus on control opportunities as a treatment plan. Considering only technical control seems to be insufficient (i.e., Email filtering solution) to reduce the number of phishing attacks. Thus, a human factor element must be considered. This can be achieved by establishing a security awareness campaign with more focus on social engineering, phishing emails, and WFH. Furthermore, a phishing simulation platform could be deployed to strengthen security awareness and training, particularly in addressing email-based threats such as business email compromise, phishing, and email-based ransomware attacks.

The new control would improve the overall Control Strength within the Trendooze environment. To estimate the effectiveness of the security awareness campaign, this control is projected that this control will impede individuals below the 90th percentile of the Threat Capability Continuum. Conversely, it is estimated that above the 96th percentile invariably succeeds, representing the extremes of this distribution. The most likely value is estimated to be the 93rd percentile. Hence, the security awareness control's effectiveness is most likely to be High as presented in Table 4.21.

Figure 4.21 demonstrates that there will be a noticeable drop in terms of ALE maximum value (from 2.2M to 804.8k) if the security awareness control is implemented. Thus, introducing a security awareness control into the Trendooze environment would improve the overall security posture by reducing the risk to an acceptable level. The rationale behind that is that the security awareness campaign has a strong resistance capability in empowering employees to take personal responsibility for protecting Trendooze's third-party IP and to enforce the policies and procedures that Trendooze has in place to protect its sensitive information.

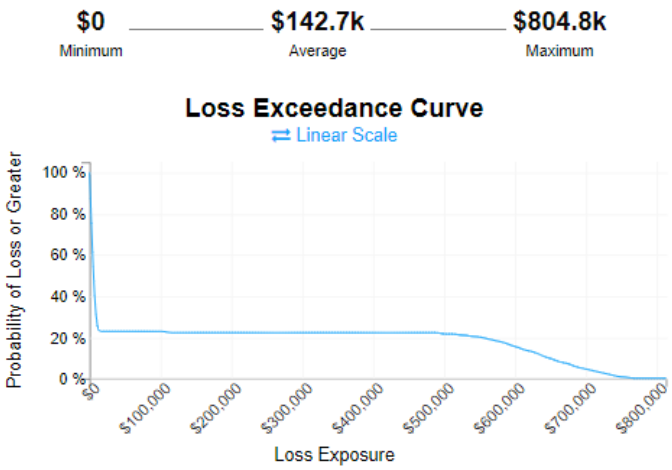


Figure 4.21: Annualised Loss Exposure after Implementing Security Awareness Campaign for Scenario 2

After defining the treatment plan, Trendooze must start thinking about which risk should be treated first. Prioritisation should be identified based on the Likelihood of risk and the Impact that was calculated in the risk estimation process. When Trendooze decided to implement the proposed additional controls to minimise the overall risk, the identified risks and their relevant components that will be monitored and reviewed.

4.2.3 Errors and Omission

It is time now to examine the results for relevance. In this scenario, the productivity loss was not a factor as there was no operational disruption affecting revenue generation, nor were there any circumstances that caused Trendooze employees to sit inactively. However, this assumption was not correct because while the Trendooze team works for months and years to create a new project and develop new inventions, cyber criminals can hack and steal their valuable work. Trendooze team might start to feel insecure and thus become unproductive.

It is common for cyber-criminal acts with little history to require updating the Threat Capability. During the scenario testing, the researcher found that in this framework there were missing components within the Risk Estimation process. In other words, this framework outlines risk management but does not offer specific details or a methodology for determining the level of risk, as depicted in Figure 4.22.

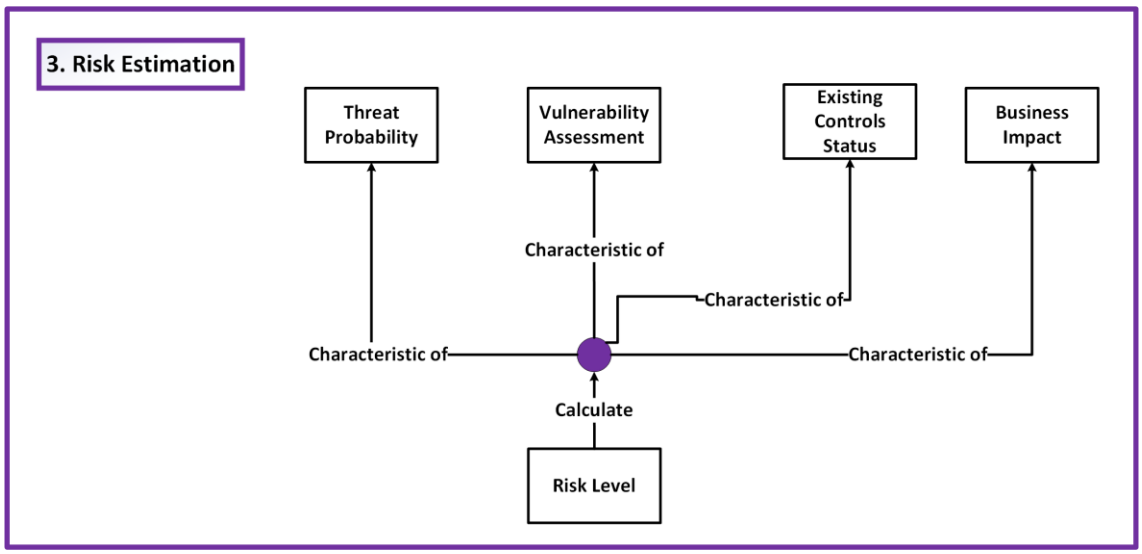


Figure 4.22: Risk Estimation Process Components

To bridge this gap, new components will need to be introduced as captured in Figure 4.23. Firstly, the risk analysts should identify Threat Action by specifying a set of activities used by a Threat Actor (e.g., insiders and cyber criminals) to create an incident scenario. These actions will be used to identify the applicable forms of loss. Secondly, the determination of Vulnerability will need two new components Threat Capability, which refers to the probable level of force that a threat actor can exert on an asset, and Control Strength, which measures the effectiveness of implemented control rather than solely considering their status. Thirdly, the Likelihood will be calculated using the Vulnerability and Threat Probability components.

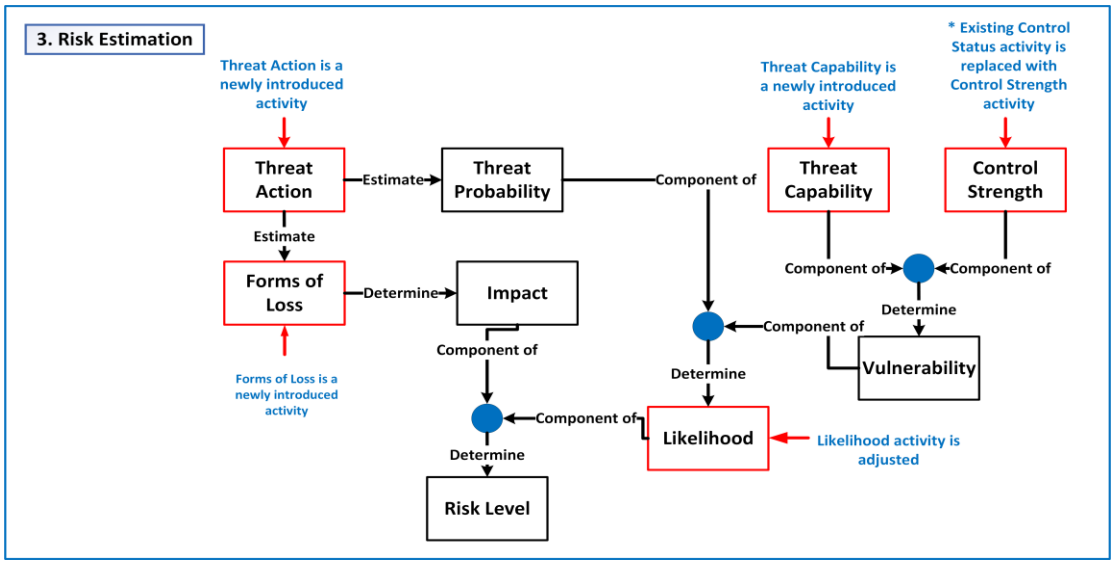


Figure 4.23: New Components Introduced to Risk Estimation Process

4.3 SCENARIO 3 – MINIMISING DATA INCONSISTENCY OF MEDICAL RECORDS

This scenario explains the implication of inconsistent medical records from a risk perceptive. Utilizing medical data, health systems can develop comprehensive perspectives on patients, and treatment approaches, enhance communication between physicians, hospitals, clinics, and patients, and ultimately improve health outcomes. Serving as a centralised repository for patient information, the Electronic Medical Record (EMR) replaces the traditional paper-based system storing patient information such as demographics, vital signs, symptoms, medications, and more.

4.3.1 Define Scenario

Medooze is a software company located in Berlin, Germany specialising in streamlined real-time clinical reporting and an EMR platform, supporting efficient patient care. Over the last five years, Medooze has undergone substantial growth, driven by its commitment to continuous innovation. Medooze employs approximately 500 employees. Around 40 employees are working in the Customer Service department, providing support to customers using the EMR platform.

Medooze recently learned that various external threats could potentially cause data inconsistency in the EMR platform, most notably data manipulation attacks. Medooze's EMR platform is made up of numerous applications and databases to store, manage, and maintain medical records. Physicians access the EMR platform either from hospitals or clinics as depicted in Figure 4.24.

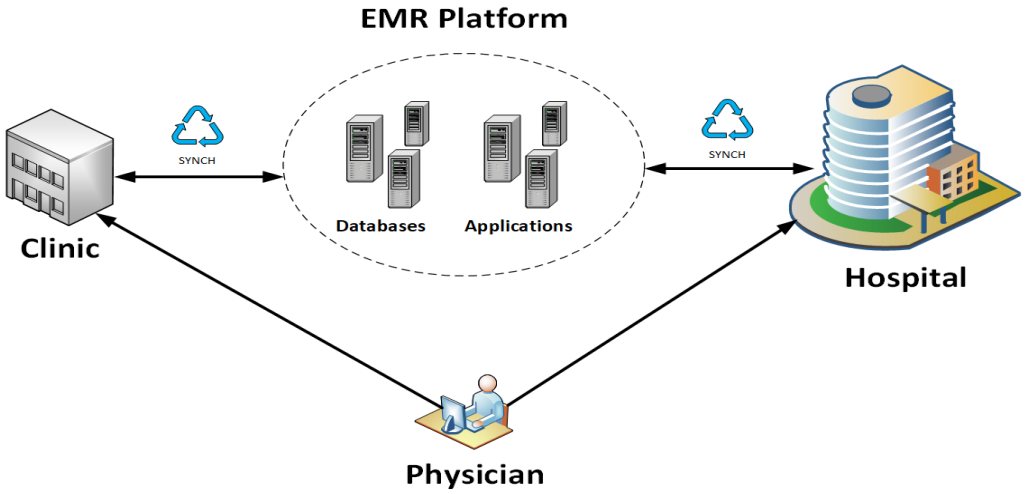


Figure 4.24: Electronic Medical Record System and Synchronisation

The EMR platform serves as a representation of the standard of care, demonstrating the consistency or potential inconsistency in treatment and policy implementation, as well as reflecting patient engagement and interaction.

The EMR process consists of various stages, including data processing, preservation, and collection. Each stage of this process carries its risks. For example, incomplete data is one of the potential risks that increase reimbursements and reduce staff-to-patient ratios, resulting in high workloads for clinicians. Staff often make inconsistent documentation because they focus on treating the patient, so documentation becomes a less priority. To mitigate the risk of data inconsistency, it is crucial to ensure the integrity and authenticity of patients' treatment records during eDiscovery. This necessitates that all clinicians make accurate and timely entries into patient records.

4.3.2 Test Artefact 1 Framework

This scenario is tested using the first artefact of the proposed framework. The next sections describe the framework's main activities along with their relevant steps.

Under pressure from the Board of Directors, Medooze's CISO is tasked with enhancing and modernising the reporting of Medooze's major risks. This is accomplished through a sequence of workshops focused on identifying these risks. During this process, both the CISO and the Security team have found that inaccurate patient information due to periodic and not real-time updates is a potential area of concern. Organised crime groups are known by Medooze to have succeeded in breaching to EMR platform and manipulating patient information in the past. This caused immediate panic in clinics and hospitals. Therefore, the CISO and his Security team have decided to conduct a risk analysis on this issue. Many health organisations are major ransomware targets, including Medooze. This means access to the EMR platform is locked until payment is made. This represents a huge risk because hospitals, clinics, and physicians rely on up-to-date information to provide patient care such as ensuring patient information is consistent. Those organisations tend to be quick to pay ransoms to regain access to the EMR platform.

The scope scenario is defined as "the malicious access and unauthorised modification of personal information by organised crime groups using data manipulation on the EMR platform". Subsequently, the scenario related to Medooze is stated as: "*Analyse the risk associated with organised crime groups impacting the integrity of patient information stored in EMR platform via ransomware attack".*

The EMR system is encrypted and required a code for accessing or reading patient health information. This encryption ensures the convenience of tracking individuals who have access to the information. As a result, the occurrence of data breaches is greatly minimised, as unauthorised access can accurately be monitored and prevented. Since the identified threat community is organised crime groups, the modification would be the most likely threat action for the EMR platform scenario. Table 4.26 presents the applicability of the six likely loss forms that will likely materialise losses from this type of scenario.

Table 4.36: Forms of Loss and their Applicability

Form of Loss	Loss Type	Applicable
Productivity	Primary	Yes
	Secondary	No
Response	Primary	Yes
	Secondary	Yes
Replacement	Primary	No
	Secondary	No
Fines / Judgments	Primary	No
	Secondary	Yes
Competitive Advantage	Primary	No
	Secondary	No
Reputation	Primary	No
	Secondary	Yes

Among the six forms of loss mentioned in Table 4.36, the most commonly experienced include Primary Productivity, Primary and Secondary Response, Secondary Fines / Judgments and Reputation. The remaining four forms of loss are not applicable in this context.

Medooze does not have a redundant EMR platform, thus previous incidents have been remedied within 3 hours. In the event of an incident, the productivity of 40 employees who provide customer support for the EMR platform would be impacted. These employees' average hourly rate is $75. Therefore, the primary productivity cost estimates are presented in Table 4.37.

Table 4.37: Primary Productivity Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
40 employees x 0.5 hrs x $75 = $1,500	*40 employees x 1.5 hrs x $75 = $4,500*	*40 employees x 3 hrs x $75 = $9,000*	*Medium*

In the case of an incident, the security team is likely to work overtime investigating and assisting incidents. Approximately 2 to 5 team members will likely work between 8 and 40 hours of overtime at a rate of $40/hr. Medooze does not normally hire an external forensic team as the current security team is very experienced in handling major incidents. Then, the primary response cost estimates are presented in Table 4.38.

Table 4.38: Primary Response Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
2 people x 8 hours x $40/hr = $640	*3 people x 24 hours x $40/hr =$2,880*	*5 people x 40 hours x $40/hr =$8,000*	*Medium*

In Table 4.39, the estimation of the likelihood of secondary loss, which refers to the percentage of primary events with secondary effects, is provided. The estimation becomes relevant to Medooze when handling scenarios involving patient information, as they would need to engage their customers if there has been a breach of their medical records.

Table 4.39: Secondary Loss Likelihood

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
95%	98%	100%	Medium

The assumptions below are required to estimate the secondary response loss:

- Medooze stores more than 100,000 customer medical records on the EMR platform. The latest report showed that 1,000 records were compromised on average.
- The cost of notifying affected customers is estimated to be approximately $15 per customer.
- Medooze has a contract in place to provide EMR platform monitoring to customers impacted by a breach. The cost is $10-20 per customer.

Table 4.40 presents the estimated costs of the secondary response taking into account all the mentioned assumptions.

Table 4.40: Secondary Response Estimates

Item	Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
Customer Notification	1 x $15 = $15	1,000 x $15 = $15,000	100,000 x $15 = $1,500,000	Moderate
EMR Platform Monitoring	100,000 x $10 = $1,000,000	100,000 x $15 = $1,500,000	100,000 x $20 = $2,000,000	Moderate
Total Cost	**$1,000,015**	**$1,515,000**	**$3,500,000**	**Moderate**

Over the past five years, fines for breaches involving customer medical records exceeding 100,000 records have varied from $20,000 to $100,000. Then, the secondary fine/judgment is estimated in Table 4.41.

Table 4.41: Secondary Fine/Judgment Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
$20,000	$60,000	$100,000	Medium

The EMR platform generates an annual revenue of $15 million, and customer contributes to an average value of $280. In the event of an incident, it is estimated that 8% of affected customers would switch from Medooze provider to another provider. This means Medooze would lose approximately 8,000 customers, and the average value of a customer is $800. Table 4.42 presents the estimated cost of the security reputation damage.

Table 4.42: Secondary Reputation Damage Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
100,000 x 2% x $4,00 = $800,000	100,000 x 5% x $600 = $3,000,000	100,000 x 8% x $800 =$6,400,000	Medium

The impact is calculated by combining both Primary Loss and Secondary Loss. Based on the previous estimations, the Impact (for most likely value) is as follows:

Impact = Primary Productivity Loss + Primacy Response Loss + [Secondary Likelihood x (Secondary Response Loss + Secondary Fine/Judgement Loss + Secondary Reputation Loss)]

Impact = $4,500 + $2,880 [98% x ($1,515,000 + $60,000 + $3,000,000)] = $4,490,880. Thus, by using Table 4.17, the Impact value is set within the High range. Recognising that the threat community is an organised crime group, it is reasonable to estimate a Moderate Threat Probability using Table 4.43.

Table 4.43: Threat Probability Ranges

Scale	Ranges
Very High (VH)	> 12 times per year (more than once every month)
High (H)	Between 6 and 12 times per year
Moderate (M)	Between 2 and 6 times per year
Low (L)	Between 0.1 and 2 times per year
Very Low (VL)	<0.1 times per year (less than once every 2 years)

Due to the scarcity of historical data, cases involving acts by organised crime groups often encounter estimations of Threat Probability, as depicted in Table 4.44.

Table 4.44: Threat Probability Estimates

Minimum (Min)	Most Likely (ML)	Maximum (Max)	Confidence
0.05 (once in 2 years)	2 (twice a year)	12 (once a month)	Medium

Using Table 4.20, the Threat Capability is estimated as follows. The most capable organised crime group sets within a Very High scale. The rationale for this estimate is that an organised crime group is more skilled and has the resources to carry out ransomware attacks.

It has been identified previously that Medooze has implemented an encryption mechanism to protect access to patient information. Encryption can effectively protect patient data during the storage (i.e., data at rest) and transmission (i.e., data in transit) states. However, encryption during the processing state within the EMR platform is generally not effective. Encryption is a strong control to protect sensitive data, but it has its limitations. The medical records are stored in an encrypted format and the data is transmitted over a secure HTTP connection. So, if we use Table 4.21 as a baseline to estimate the Control Strength, then the Moderate scale would be a right fit. The reason is that encryption control will not prevent organised crime groups from blocking files if a ransomware attack occurs. When a Very High Threat Capability and a Moderate Control Strength are combined, the Vulnerability resulting is Very High based on Figure 4.8.

In this scenario, given a Threat Probability of Moderate and Vulnerability of Very High, the Likelihood is Moderate based on Figure 4.9. The Impact score is compared to

the Likelihood that can be determined. Given an Impact of High and a Likelihood of Moderate, the Risk Level is High based on Figure 4.10. The results of the analysis are presented in Table 4.45 which shows the estimates entered into the FAIR-U tool.

Table 4.45: Risk Components for Organised Crim Group Ransomware Attacks

Scenario 3 - Minimising Data Inconsistency of Medical Records

Purpose	Asset	Threat Community	Threat Type	Threat Effect
Analyse the risk associated with organised crime groups impacting the integrity of patient information stored in EMR systems via a ransomware attack	EMR Platform	Organised Crime Group	Malicious	Integrity

Primary Loss	Min	ML	Max	Confidence
Productivity	$1,500	$4,500	$9,000	Medium
Response	$640	$2,880	$8,000	Medium
Replacement	$0	$0	$0	Medium
Competitive Advantage	$0	$0	$0	Medium
Fines and Judgments	$0	$0	$0	Medium
Reputation	$0	$0	$0	Medium

Secondary Loss	Min	ML	Max	Confidence
Productivity	$0	$0	$0	Medium
Response	$1,000,015	$1,515,000	$3,500,000	Medium
Replacement	$0	$0	$0	Medium
Competitive Advantage	$0	$0	$0	Medium
Fines and Judgments	$20,000	$60,000	$100,000	Medium
Reputation	$800,000	$3,000,000	$6,400,000	Medium

	Min	ML	Max	Confidence
Likelihood (Frequency of Events)	0.05	2	12	Medium
Secondary Likelihood	95%	98%	100%	Medium
Threat Capability	2%	84%	98%	Medium
Control Strength	60%	78%	90%	Medium

Figure 4.25 and Figure 4.26 illustrate the simulation output depicting the analysis above. The screenshot displays the resulting ALE derived from the estimated probable frequency (Likelihood) and probable future loss (Impact) for this given scenario.

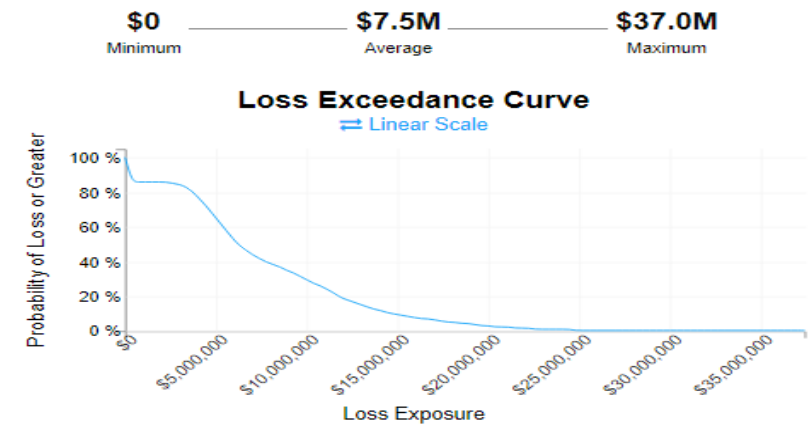


Figure 4.25: Annualised Loss Exposure with Linear Scale for Scenario 3

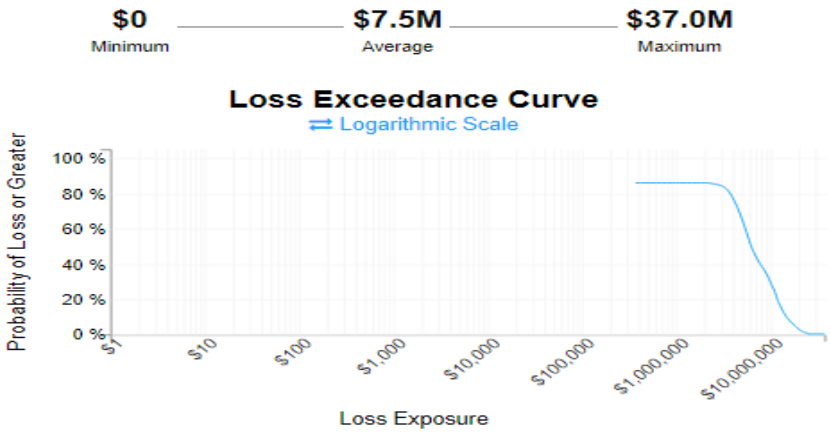


Figure 4.26: Annualised Loss Exposure with Logarithmic Scale for Scenario 3

Table 4.46 details the results of the simulation based on the estimated variable inputs. The data presented include the projected annual frequency of Primary Loss events and their corresponding monetary losses, the projected annual frequency of Secondary Loss and their respective monetary losses, as well as the resulting ALE.

Table 4.46: Summary of Simulation Results for Scenario 3

Primary

	Min	Avg.	Max
Likelihood (Loss Events / Year)	0	1.52	5
Impact (Loss Value)	$2.6k	$8.2k	$14.4k

Secondary

	Min	Avg.	Max
Likelihood (Loss Events / Year)	0	1.49	5
Impact (Loss Value)	$2.2M	$5.0M	$8.9M

Vulnerability 45.59%

The $7,500,000 is a high value because ransomware attacks are complicated, and this value could go up to $37,000,000. This average value can be considered a High risk and typically treated as such by introducing another strategy to mitigate the exposure. No software will be able to unblock the encrypted files or records, so another control needs to be considered to protect patient information before a ransomware attack happens. Paying for ransomware once can encourage the organised crime group to try again. To combat and protect patient information against ransomware, Medooze must have data copied, protected, and safely stored in a separate environment that has limited access. Having this additional control helps Medooze to recover the lost data once a ransomware attack occurs.

The data backup and recovery control improve the overall Control Strength within the Medooze environment. In order to estimate the effectiveness of the data backup and recovery system, this control is anticipated to prevent any individuals below the 90th percentile along with the Threat Capability Continuum from succeeding. It is also estimated that individuals above the 96th percentile are highly likely to succeed. The most likely value is estimated to be the 93rd percentile, indicating that the backup control's effectiveness is most likely to be High (as referenced in Table 4.21).

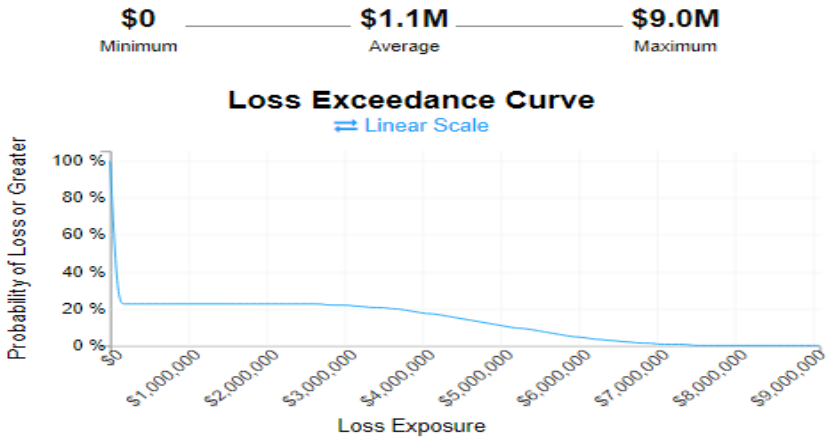


Figure 4.27: Annualised Loss Exposure after Implementing Data Backup and Recovery for Scenario 3

Figure 4.27 clearly shows that there will be a big reduction in terms of the ALE maximum value (from 7.5M to 1.1M) if the data backup and recovery control is implemented. In other words, implementing the data backup and recovery control into the Medooze environment introduces change by minimising the current risk to an acceptable level. The rationale behind that is that the data backup control has a strong resistance

capability in restoring ransomware-encrypted files or records, rather than paying the organised crime group ransom. A specialised ransomware decryption tool could be considered as another strategy that will simply break the ransomware encryption placed on the EMR platform. The same approach would be followed to recalculate the ALE value (i.e., reassess the Control Strength).

After defining the treatment plan, Medooze must start thinking about which risk should be treated first. Prioritisation should be identified based on the Likelihood of risk and the Impact that was calculated in the risk estimation process. Upon deciding to implement the suggested controls, Medooze aims to mitigate the overall risk. Consequently, it is important to monitor and review the identified risks and their relevant components.

4.3.3 Errors and Omission

The ALE result is still too high (i.e., the maximum value is 1.1 M) even after considering an effective control (i.e., data backup and recovery). This occurs when the Likelihood or Vulnerability is not realistic. Threat Probability values for Medooze are relatively high, ranging from once every 2 years to every month. This is primarily due to their focus on digital medical records services and their avoidance of raising funds through their web or running their e-Commerce site. However, the assessment of Competitive Advantage loss was omitted as it is recognised as one of the most challenging factors to evaluate. If Medooze has a unique patent or copyright that distinguishes them from other organisations, Medooze can gain a Competitive Advantage over them.

During the scenario testing, the researcher found there is a mathematical relationship between various components of the risk management framework. For instance, the primary response loss cost involves several costs including the effort cost of internal teams (e.g., hourly rate) dealing with the incident as well the consultancy cost of the external forensic team who will support Medooze during the incident. These costs may vary based on different factors, including internal team capability, the business impact, the scope of incident response, and other unexpected circumstances. It is important to understand the impact of an incident (i.e., incident priority) by measuring the effect of an incident, change, or issue on the day-to-day Medooze business activities. This could include but not be limited to the number of users or customers impacted, the cost incurred in incident resolution, and the number of systems or services involved. However, the functional relationships between various factors will be elaborated more in the next section.

4.4 ARTEFACT 2

An iteration process has been carried out to ensure that the recommended changes applied to the new version of the proposed artefact are linked with the previous version. The feedback from the testing function is used to improve the proposed framework and create Artefact 2 as illustrated in Figure 4.28. The green boxes represent the new components introduced to the proposed framework that contributed to overall improvement.

The following subsection provides specific details about the major differences between Design 1 and Design 2 in terms of changes and adjustments made to improve the proposed risk management framework.

4.4.1 Artefact 1 and Artefact 2

The principles in both Artefact 1 and Artefact 2 are the same. Similarly, the activities in the Context Establishment remain as they are. During the scenario testing, the researcher found that the Assets Valuation activity did not fit with the FAIR model as part of the Risk Identification process. Instead, Data Mapping was introduced as an activity that has a centralised inventory listing of what types of ESI an organisation has and where they are stored. This mapping was also a key output when creating a DFD and BPM.

There were major changes/adjustments applied to the Risk Estimation process. This represents a core improvement of Artefact 1 due to the introduction of the FAIR model. Artefact 1 does not offer specific details or a defined approach for managing risk or determining risk levels. On the other hand, the FAIR model presents a methodology that enables the identification and quantification of risks, meaning it provides a concrete framework for evaluating the probabilities and impacts of real risks. As presented in Figure 4.28, the new components have been added to Artefact 2. These are Threat Action, Threat Capability, Forms of Loss, Control Strength, and Likelihood (i.e., coloured in green boxes).

The FAIR model serves as an analytical framework for understanding the factors that influence the frequency and magnitude of loss. It provides a clear definition of these factors and their interrelationships. For example, consider the formula for measuring speed, Speed = Distance / Time. In this equation, the factor involved (distance and time) are identified, along with the way they are combined (distance divided by time). Similarly, the FAIR model establishes a structured understanding of the factors driving risk (Jones, 2019).

Incorporating the FAIR model into Artefact 2 establishes a structured framework and methodology for the analysis and evaluation of risks. This integration brings significant enhancement, particularly in terms of combining security risk management with the modified FAIR model components. Hence, Figure 4.28 addresses the key activities (as addressed in Artefact 1) with the quantification capabilities offered by the FAIR model (as addressed in Artefact 2). The result is a more comprehensive and robust approach to risk assessment and management.

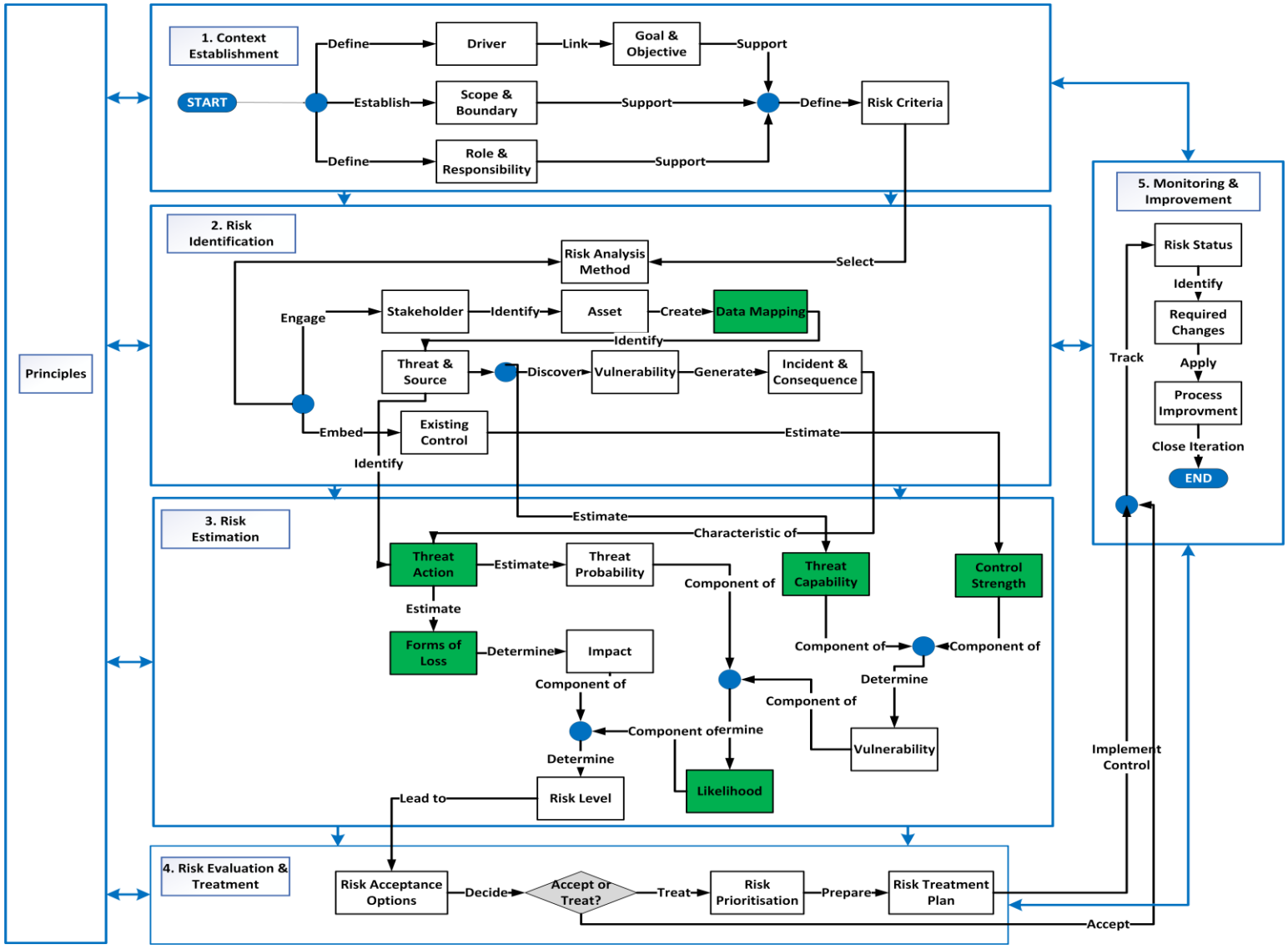


Figure 4.28: Security Risk Management Framework (Artefact 2)

The new changes and adjustments to improve Design 1 are summarised as follows:

- Threat Action is a key activity to estimate Threat Probability and Forms of Loss.
- Design 1 does not provide detailed steps on how to assess Vulnerability.
- Design 2 introduces a new key component Threat Capability and replaces the Existing Control Status with Control Strength to align with the FAIR model ontology.
- The Likelihood is clearly defined in Design 2 as a key component to estimate the overall Risk Level.

The changes/adjustments above offer two key benefits to the overall risk management framework:

- A better understanding of components (factors) contributing to risk calculation.
- Ability to better troubleshoot analysis performed at higher layers of abstraction.

The last note here is that Design 2 does not propose any change to the Risk Evaluation and Treatment activity and Monitoring and Improvement activity because they cover the risk management aspects rather than the risk estimation/calculation aspects. From an improvement perspective, the following subsections suggest a metamodel for the proposed risk management framework using the ArchiMate 3.1 design tool. In this metamodel, all concepts and components were converted from Artefact 1 presented and explained previously in Chapter 3. Finally, the proposed Artefact 2 model is used and architected in the ArchiMate 3.1 modelling tool.

ArchiMate 3.1 provides a comprehensive architecture modelling language with graphical notation, relationships, and metamodels per the six layers of the emerging architecture including Strategy, Business, Application, Technology, Physical, and Implementation Migration as well the four aspects/views including Passive Structures, Behavior, Active Structures, and Motivation. In this research, two layers, Strategy and Business, are used to represent the security additions for practice.

In order to design a metamodel for the proposed risk management framework using ArchiMate 3.1, it is important to establish a mapping between the concepts and components of the framework with ArchiMate 3.1 concepts, as illustrated in Figure C1.1,

Figure C1.2, Figure C1.3, and Figure C1.4 in Appendix C1. This will be further discussed in the subsequent sections.

4.4.2 Security Risk Management Framework with ArchiMate 3.1 Metamodel

In this section, the researcher employed an ArchiMate 3.1 metamodel as a complementary method to the textual description of the security risk management framework to model the proposed Artefact 2.

4.4.2.1 Framework Modeling

Visual information offers a clearer means of representation, particularly when dealing with complex and unstructured subject matter. It facilitates the elimination of ambiguous knowledge and information, enabling the researcher to generate, retrieve, elicit, restructure, evaluate, locate, and access information more effectively (Almeida et al., 2019).

The proposed metamodel in Figure 4.29 formulates two layers: strategy and business. The remaining layers were not presented because this metamodel focuses on process and people. These layers incorporate nearly all the pertinent behavioural and structural components of the proposed risk management system for businesses. Figure 4.29 identified the assets of significant value and the components in which that value is protected. For each component, a set of Business Goals are identified (i.e., they are linked to the key principles) that are necessary to improve or protect the value (SABSA, 2021). For each Business Goal, the risk assessment process (risk identification and estimation) consists of various actions:

- A Threat Analysis to identify threats to the Business Goal.
- A Vulnerability Analysis to identify weaknesses in Assets that could expose their value to this Threat.
- An Impact Analysis to assess the loss of Asset Value (Forms of Loss) that the Threat to the Vulnerability should occur.

The risk assessment considers the Threat Probability, the exposure of the Vulnerability and the Impact to estimate the risk level (ALE). An influence relation is depicted here to reflect the analysis direction. On the other hand, in the risk evaluation and treatment process, the Owner of the Business Goal (e.g., management, board of directors) must decide whether to accept, treat, transfer, or avoid the identified risk (i.e., modelled as Outcomes).

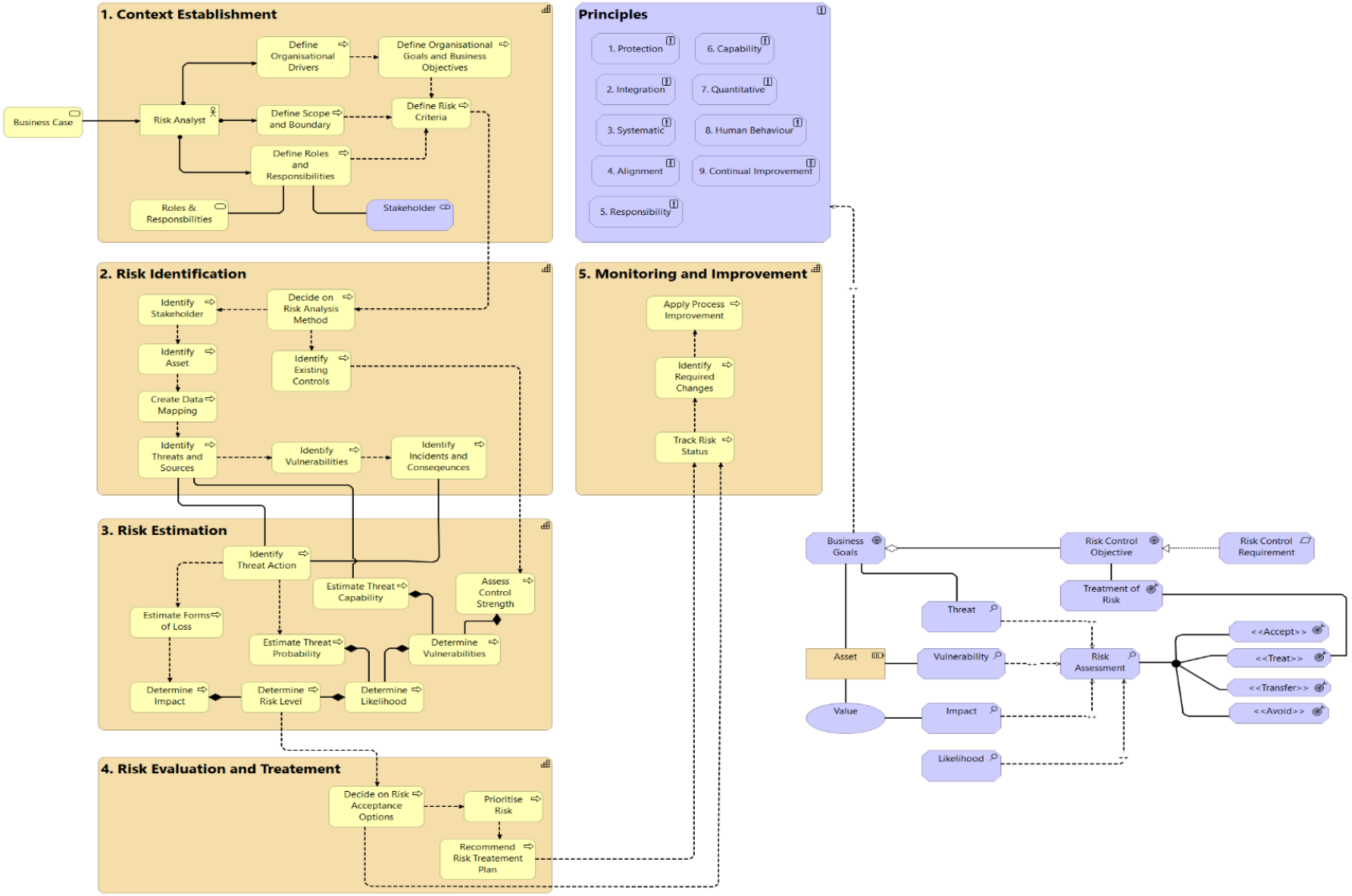


Figure 4.29: Proposed Security Risk Management Framework with ArchiMate 3.1

4.4.2.2 Derive Risk Formulas

The proposed security risk management framework comprises a set of functions that pertain to variables (risk factors). These functions aim to statically or probabilistically depict the functional connections between a factor and its respective sub-factors (Wang et al., 2020). These factors and their associated functions are presented and summarised in Table D1.1 in Appendix D1.

The risk assessment through the proposed framework has two key procedures: determining impact by aggregating Primary Loss and Secondary Loss and determining Likelihood by calculating Vulnerability and estimating Threat Probability. By employing a Monte Carlo simulator to simulate samples for input factors, and subsequently manipulating these samples according to their corresponding functions. Subsequently, the ALE or Risk Level can be estimated. Figure D1.1 in Appendix D1 illustrates a mind map for Forms of Loss subcomponents and provides common input factors required to estimate both Primary and Secondary Loss. This list was extracted and then formulated to represent various variable choices.

4.5 CONCLUSION

Scenario tests are used in the first iteration of improving the Strawman design. The Strawman (Artefact 1) has been applied to each diverse scenario to evaluate their strengths, weaknesses, errors, and omissions. Several criteria were taken into account when selecting a scenario approach to apply the proposed framework described in Chapter 3. These criteria encompassed the requirement for empirical testing of the research questions, the complexity of the expected outcomes, and the need to work within the limitations of time, budget, and information accessibility. The adoption of a scenario approach was chosen because it provided access to real-life information.

To test the proposed security risk management framework, this chapter presents three disparate scenarios of an Energy Provider, an IT Service Provider, and a Health Care Service Provider respectively. The introduction of these scenarios serves to strengthen the concepts and methodologies that have been presented in the previous chapters. Initially, an informal description of a scenario was provided, followed by a comprehensive list of prerequisites for each scenario. Secondly, each scenario was tested on Artefact 1 as the proposed framework. Thirdly, the final results were examined to correct errors and omit any wrong data. An iteration process has been identified to ensure

that the recommended changes applied to the new version of the proposed Artefact 2 are linked with the previous version. The feedback from the testing function was used to improve the proposed framework and create Artefact 2.

ArchiMate 3.1 tool was used to create an architecture modelling of the Artefact 2. This was represented in a set of graphical notation, relationships, and metamodels per two selected layers of the emerging architecture: Strategy and Business, as well as four aspects/views including Passive Structure, Behavior, Active Structure, and Motivation. The proposed security risk management framework comprises a set of functions that are connected to variables (risk factors). These variables represent the functional relationships between a factor and its corresponding sub-factors, either statically or probabilistically. The factors and their associated functions are determined through a series of formulas.

Finally, this chapter presents the improved version of the proposed framework Artefact 2. It is communicated to the selected experts for evaluation and subsequently reported in Chapter 5. Therefore, Chapter 5 discusses the results of two types of evaluation: naturalistic expert evaluation and Artefact thematic evaluation, and then presents the next improved version of the proposed framework Artefact 3.

Chapter 5: Artefact 2 Expert Feedback

5.0 INTRODUCTION

Figure 5.1 illustrates the summary of the thesis structure based on the proposed research methodology. The dashed lines show the roadmap for Chapter 5 which is Phase 5 (Demonstration Effectiveness Evaluation).

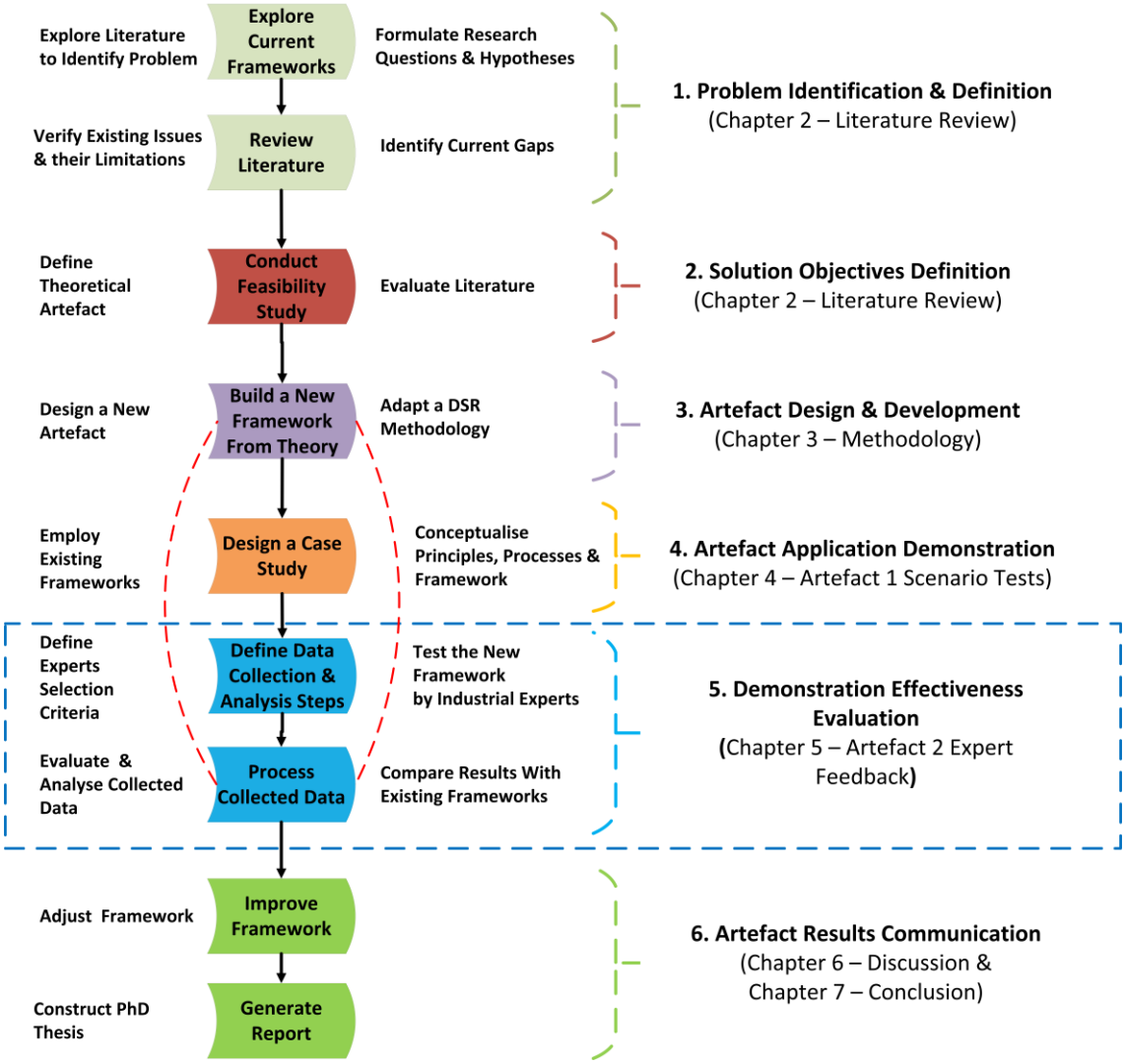


Figure 5.1: Chapter 5 Roadmap

Each DS artefact produced as an output can be subjected to an improvement process based on expert feedback and testing processes. The evaluation process incorporates expert feedback as an iterative improvement cycle and is a major part of each application phase of the DSM. Chapter 5 focuses on presenting and analysing expert feedback on the proposed Artefact 2 and then applying changes to reach the target Artefact 3 output.

This chapter is organised as follows. Section 5.1 provides an overview of artefact evaluation types in the context of this research. Section 5.2 reports the naturalistic evaluation activities, including fieldwork and evaluation preparation. It also covers a full spectrum of expert feedback on the proposed framework, and the researcher's reflections and suggested changes. Moreover, this section records the expert feedback and then analyses the results of the proposed artefact improvement from various criteria, including its efficacy, clarity, usefulness, alignment, usability, robustness, improvability, and completeness. Section 5.3 reports the artefact thematic evaluation using the NVivo tool.

Section 5.4 provides a roadmap to improve Artefact 2 based on expert feedback. Thus, Section 5.5 is dedicated to highlighting the major differences between Artefact 2 and Artefact 3 in terms of changes and adjustments made to improve the proposed security risk management framework. This improvement is captured through various dimensions including integration between the eDiscovery process and the proposed framework as well as framework principles, style, process, and architecture model. Chapter 5 ends with a summary of the main points and connection to Chapter 6 in Section 5.6.

5.1 ARTEFACT EVALUATION

The evaluation of the Artefact aims to assess the extent to which it fulfils the requirements and effectively addresses the identified problem that served as the motivation for the research (Johannesson & Perjons, 2014). The evaluation process involves two main stages: naturalistic evaluation and thematic evaluation. The examination of the investigation's test data was conducted critically, and the feedback received from experts was carefully considered to enhance the framework and develop a comprehensive guideline.

5.2 NATURALISTIC EXPERT EVALUATION

Naturalistic evaluation involves a real test in which the proposed artefact is assessed within an authentic environment to evaluate its effectiveness and efficiency. This type of evaluation is particularly suitable for examining the effectiveness of the artefact. Naturalistic evaluations offer robust external validity as they are carried out in genuine settings, allowing the results to be generalised or applied to similar situations (Johannesson & Perjons, 2014).

Based on the literature discussed in Section 3.4.2.3, various numbers of respondents were suggested, ranging from 4 to 30. However, the researcher ultimately opted for 10 respondents, as this aligns with the average recommendation made by (Hevner & Chatterjee, 2010). The rationale behind this choice is rooted in the need to account for the experts' enthusiasm for the subject and their commitment to actively participate and provide feedback for the validation and enhancement of the Artefact 2. This number is considered sufficient based on the reviewed literature and serves to make both data collection and analysis more manageable. While it is acknowledged that this number can be adjusted, the researcher prioritised ensuring that the results would remain manageable for the data collection and analysis processes, and also to foster the participation of these scarce experts. Obtaining contributions from experts in this research proved to be challenging during this study. The researcher sent more than 10 invitation letters and got replies from all of them. Naturalistic evaluation has been conducted, and 10 competent experts have been approached, thereby ensuring that different perspectives and interests were captured.

Those experts were contacted and granted approval to evaluate the artefact using the ADSRM approach outlined in Section 3.4. Those experts came from various fields, including security risk management and security investigation. The evaluation process was designed to involve numerous experts throughout the assessment, so accurate results can be obtained.

5.2.1 Fieldwork Activities

Selected experts were contacted to participate in evaluating the proposed artefacts from the ISACA database. Those experts were selected from the professional network of the local community in New Zealand and were qualified to reflect on professional practice in eDiscovery, and security and risk management.

ISACA, a reputable association in IT governance and cybersecurity vets its members and experts. ISACA membership requires meeting education, experience, and certification criteria, as well as providing references. Members must also maintain ongoing professional development. ISACA verifies member's credentials and measures credibility and expertise through recognition in the community.

The researcher designed a feedback template that consists of 8 multiple choice questions and 2 open questions. These questions have been chosen after considerable evaluation to ensure that any responses are useful to the research. The feedback template was communicated to 10 experts specialised in risk management, and a brief verbal

explanation was given of the framework. The majority of participants had many years of experience in this field. Each expert has specialised skills in different fields as described in Table 5.1.

Table 5.1: Experts Profile

Practitioner Code	Role	Experience
Expert 1	Technology Manager	5 Years
Expert 2	Senior Security Engineer & Information Security Manager	+25 Years
Expert 3	Secure Software Developer	18 Years
Expert 4	Digital Forensic Analyst	9 Months
Expert 5	Academic Member of Staff	10 Years
Expert 6	Security Consultant	12 Years
Expert 7	Cybersecurity Consultant and Risk Management Practitioner	+10 Years
Expert 8	Information Security Consultant	22 Years
Expert 9	Information Security Manager	+7 Years
Expert 10	Cyber Security Manager	21 Years

The selected experts were ISACA members and have experience in risk control framework implementation and security management (e.g., ITIL, COBIT, and TOGAF) as well as full security lifecycles, including the ISO/IEC 27001 standard. Furthermore, many of the selected experts have been involved in security incidents investigation engagements and eDiscovery processes.

5.2.2 Evaluation Preparation Activities

A set of files were given to the experts as part of the Artefact evaluation guidance. These included an introduction letter, the developed Artefact, and a list of questions. They were communicated to the experts via email as explained in the subsections below.

5.2.2.1 Introduction Letter

An introduction letter was created to start building professional connections with the experts as shown in Appendix A2. It was a written correspondence that explains who the researcher is and provides the experts with the context and information they need to participate in the research evaluation and feedback.

5.2.2.2 Artefact

A copy of the proposed security risk management framework diagram (Artefact 2) shown in Figure 4.28 was shared with the experts. This diagram explains the workflow process of the proposed framework with relevant activities.

5.2.2.3 A List of Questions

A template was used as a research instrument that consists of a set of questions guides that aim to collect feedback from the experts (refer to Appendix A3).

In this research, a mixture of close-ended and open-ended questions was designed. The close-ended questions provide the experts with predetermined answers, while the open-ended questions enable the experts to respond using their own words. The experts could also add more free feedback and provided their feedback through email. The researcher has defined 8 evaluation criteria along with their corresponding questions as outlined in Table 5.2. During the questions template design, the researcher has pre-coded questions for later statistical analysis. This made the subsequent data entry easier and less susceptible to error.

Table 5.2: Evaluation Criteria for Expert Feedback

No.	Evalaution Critiera	Question
-	Responsibility	What is your role?
-	Experience	How long you have been in the industry?
1	Efficacy	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?
2	Clarity	Are the defined components of the proposed artefact clear and relevant to what you observe?
3	Usefulness	How useful is the proposed artefact for your workplace?
4	Alignment	Does the proposed artefact align with the international security risk management standards?
5	Usability	Is it usable?
6	Robustness	Will it improve risk management?
7	Improvability	Should the artefact be improved?
8	Completeness	Should modifications be made to any component of the proposed artefact?

No.	Evalaution Critiera	Question
9	Advantages	List strengths.
10	Disadvantages	List weaknesses and improvements.
-	Open Feedback	Any other comments

Regarding expert feedback, all information has been acquired from Microsoft Word documents and transformed into corresponding spreadsheets. Moreover, a sanitisation procedure has been implemented to safeguard and maintain the confidentiality of the personal data belonging to the experts. The significant insights derived from the expert evaluation have been presented in various formats suitable for naturalistic and thematic evaluation approaches.

5.2.3 Experts' Evaluation

To examine the average opinion of the experts, a set of questions were devised that could be easily answered using a Likert scale, which offers straightforward response options. This Likert scale was used to measure the quality of the artefact components. It is used to allow the experts to indicate their positive-to-negative strength regarding the questions. The researcher used a **5-Level Likert Scale** with the following scale items: **1 = Excellent, 2 = Good, 3 = Ok, 4 = Poor, and 5 = Change**.

The Likert scale is a type of psychometric response scale that enables experts to indicate their level of agreement with a statement. It offers the advantage of capturing nuanced opinions instead of simple binary (Yes / No) responses, allowing for varying degrees of agreement or even the absence of an opinion. This approach yields quantitative data, facilitating easy analysis. For each question, responses were plotted to illustrate the variations among the five scales employed in the expert feedback.

Regarding the open feedback, the experts were specifically inquired about the strengths, and weaknesses of the proposed artefact. Furthermore, they were asked to identify components that could be improved and provide such enhancements that could be implemented (i.e., specifically addressed in questions 9 and 10 respectively). The descriptive statistics were then computed based on the responses received. The researcher obtained the mean score for each question as follows: +2 = 'Excellent', +1 = 'Good', 0 = 'Ok', -1 = 'Poor', and -2 = 'Change'. The mean score in the proximity of +2 indicates that the experts rated a feature (e.g., efficacy) as 'Excellent' whilst a -2 indicates that they think this feature requires "Change' as shown in Figure 5.2.

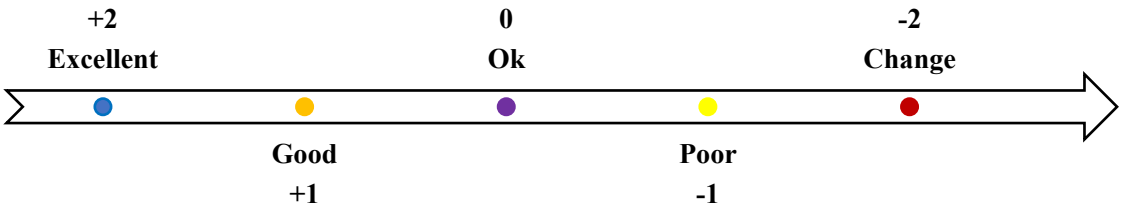


Figure 5.2: 5-Level Likert Score

In terms of expert feedback, the gathered data were extracted from the spreadsheet and presented in a tabular layout. Care was taken to maintain the anonymity of the experts' identities during this process. The feedback text underwent editing to correct any typographical errors if required. Within the experts' feedback, any unanswered questions were specifically highlighted using yellow colour.

During the initial data collection, the researcher gathered feedback from 5 experts, analysed the emerging themes, and evaluated the data for saturation. Following feedback from 10 experts, the researcher verified that data saturation has been achieved and subsequently ceased further data collection.

5.2.3.1 Expert 1

Expert 1 has 5 years of experience and works as a Technology Manager for a banking institute. Expert 1 comments are analysed in Figure 5.3.

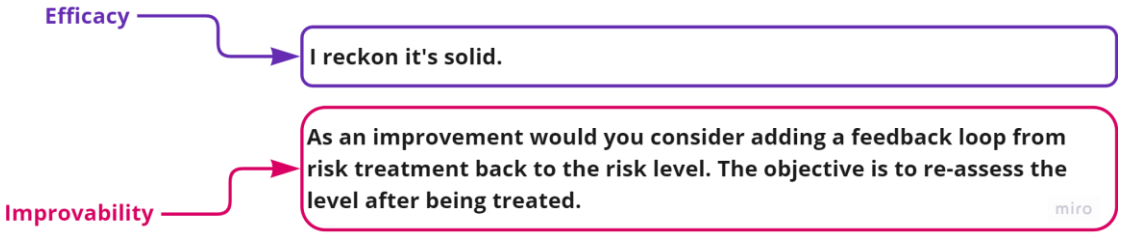


Figure 5.3: Expert 1 Comments Analysis

As outlined in Figure 5.4, Expert 1 indicated that the proposed artefact would be a good fit framework for eDiscovery risk management and agreed that it could be improved in the future (value = +1). However, Expert 1 evaluated its relevancy, usefulness, possibility to improve risk management, and required modifications (value = 0). On the other hand, Expert 1 did not score both the Alignment and Useability criteria for the proposed artefact.

The overall scoring of Expert 1 feedback was **0.33** which sets between 0 and 1. That means the proposed artefact could be fit for purpose if a minor modification is made to its components.

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
1	0	0	N/A	N/A	0	1	0

Figure 5.4: Evaluation Criteria Scores Provided by Expert 1

Expert 1 thought that the proposed framework is solid. Adding a feedback loop from the Risk Evaluation & Treatment (Phase 4) back to the Risk Level component (i.e., the last step in the previous phase), the Risk Estimation (Phase 3) would be improved as illustrated in Figure 5.5. The rationale behind that is to re-assess the Risk Level after being treated.

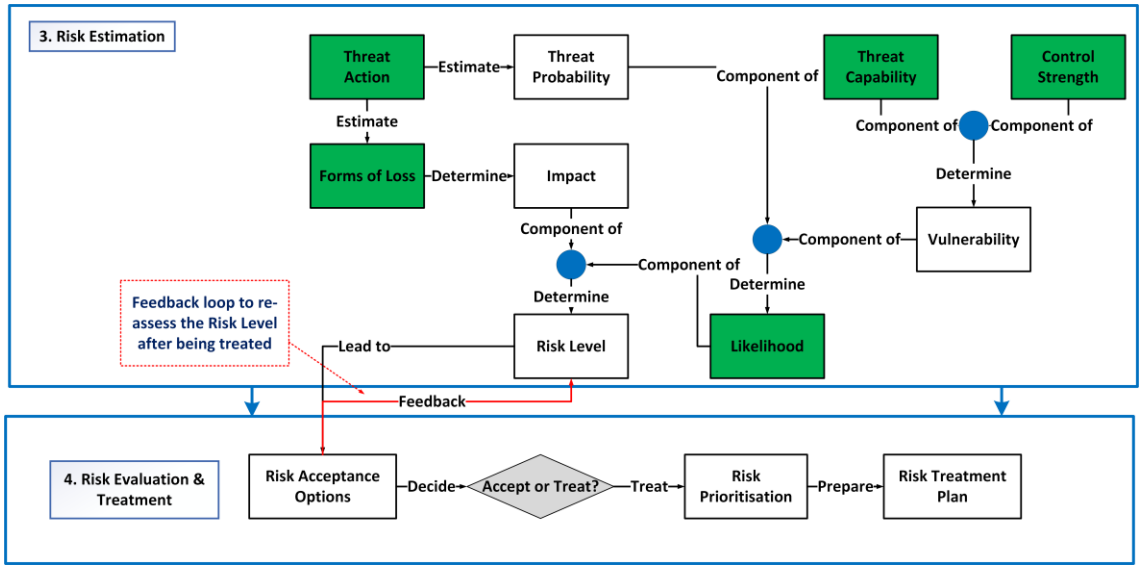


Figure 5.5: Proposed Improvement Provided by Expert 1

5.2.3.2 Expert 2

Expert 2 has more than 25 years of experience and works as a Senior Security Engineer as well as an Information Security Manager. Expert 2 comments are analysed in Figure 5.6.

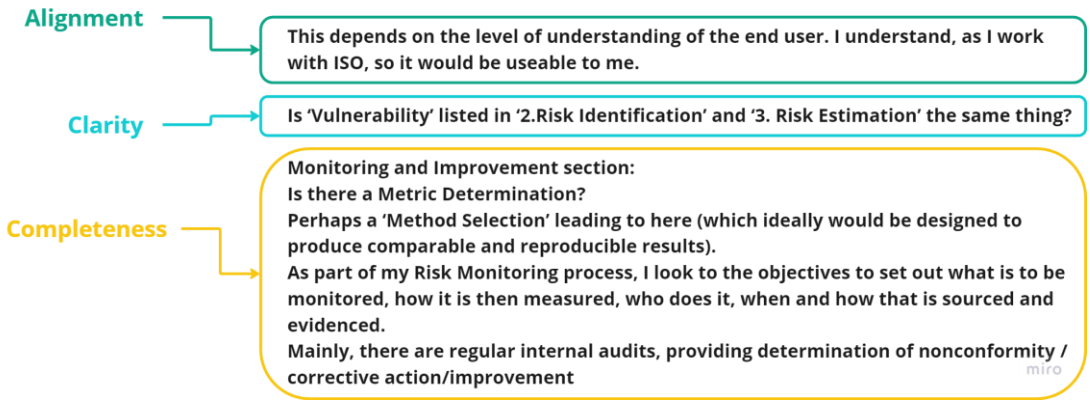


Figure 5.6: Expert 2 Comments Analysis

As described in Figure 5.7, Expert 2 thought that the proposed artefact has a good quality in terms of its efficacy, clarity, and alignment with international security risk management standards (value = +1). Additionally, it could be a useful framework depending on the level of end-user understanding (value = 0). Moreover, this framework will improve risk management for a specific use such as e-discovery risk (value = +1).

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
1	1	0	1	0	0	0	0

Figure 5.7: Evaluation Criteria Scores Provide by Expert 2

On the other hand, Expert 2 believed that the proposed artefact needs to be improved as outlined in Figure 5.8 (value = 0).

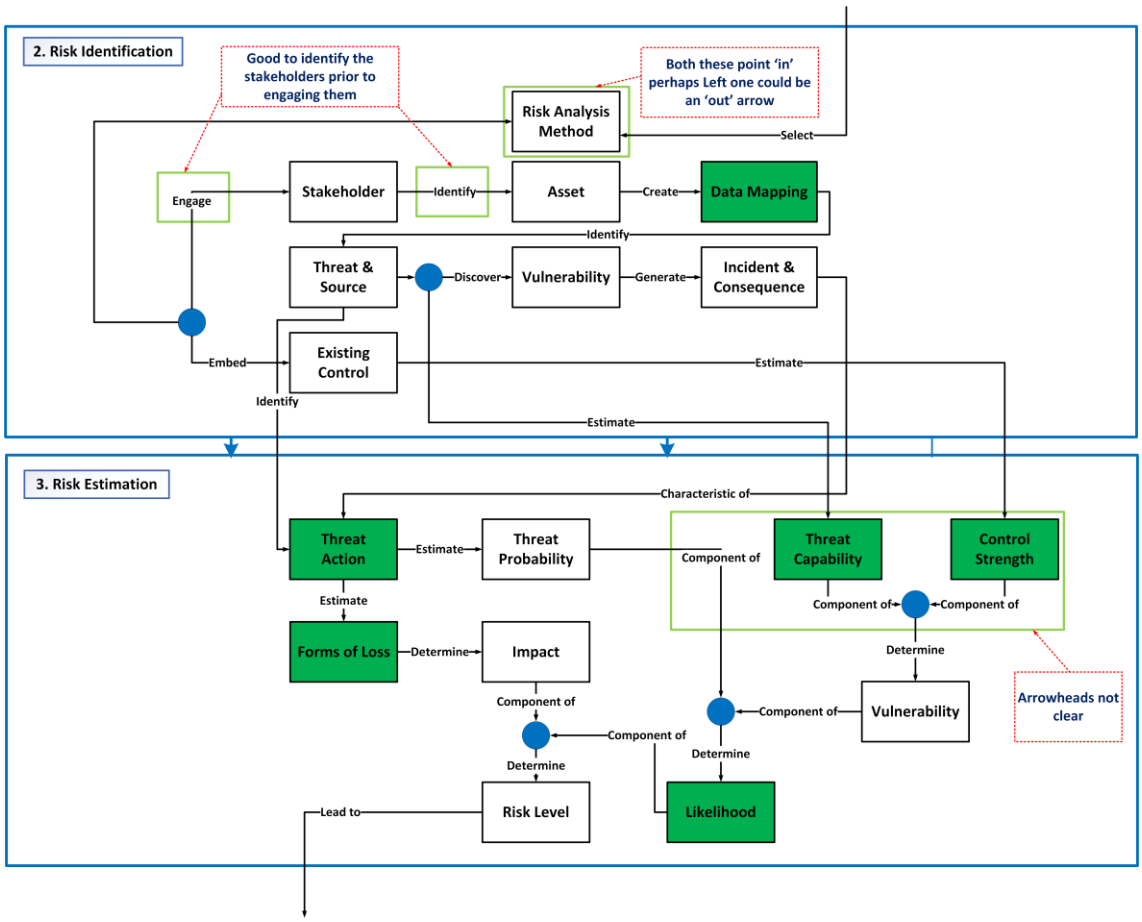


Figure 5.8: Proposed Improvement Provided by Expert 2

Expert 2 provided three observations about the workflow of the proposed artefact (value = 0):

- Adding a new activity to identify the Stakeholders before engaging them in the Asset identification task.
- The arrow on the Left side of the Risk Analysis Method should be an 'out' rather than 'in'.
- Arrowheads coming out and coming in both Threat Capability and Control Strength components are not clear (i.e., the current diagram does not show the arrowheads are either in or out.

Expert 2 reported that the proposed artefact is clean and clear which is considered one of its strengths. However, Expert 2 raised a few questions that might help improve the quality of the proposed artefact:

- Is "Vulnerability" listed in both Phase 2 Risk Identification and Phase 3 Risk Estimation the same?
- Is there a "Metric Determination" within Phase 5 Monitoring & Improvement?

Expert 2 commented that perhaps a 'Method Selection' leading to here (which ideally would be designed to produce comparable and reproducible results). As part of the Risk Monitoring process, Expert 2 looked at the objectives set out:

- What is to be monitored?
- How is it then measured?
- Who does it? When and how that is sourced and evidenced?

Expert 2 stated that there should be regular internal audits, providing a determination of nonconformity and corrective action/improvement. The overall scoring of Expert 2 feedback was approximately **0.4 (positive)** which sets between 0 and 1 (positive). That means the proposed artefact could be fit for purpose if minor modifications are made to its components.

5.2.3.3 Expert 3

Expert 3 works in the Secure Software Development area with 18 years total of experience. Expert 3 comments are analysed in Figure 5.9.

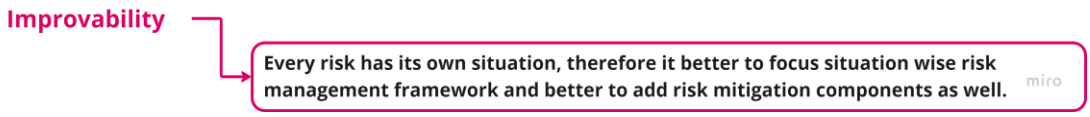


Figure 5.9: Expert 3 Comments Analysis

Expert 3 provided an 'Ok' score for the efficacy, usefulness, alignment, and completeness of the proposed artefact (value = 0). Expert 3 observed that the proposed components of the artefact are not clear and not relevant to the research context (value = -1). In addition to that, Expert 3 indicated that the proposed artefact is not useable and cannot be improved at this stage (value = -1). The scores above are recorded in Figure 5.10.

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
0	-1	0	0	-1	0	-1	0

Figure 5.10: Evaluation Criteria Scores Provided by Expert 3

On the other hand, Expert 3 believed that the proposed artefact did not have any strengths. In terms of weaknesses and improvements, Expert 3 suggested that every risk has its situation; therefore, it is better to focus on situation wise risk management framework and better to add Risk Mitigation components as well.

Expert 3 did not provide any further comments. Hence, the overall scoring of Expert 3 feedback was approximately **- 0.4 (negative)** which sets between 0 and -1 (negative). That means the proposed artefact is 'Poor' in terms of its quality and required key modifications made to its shape, so the improved version could be fit for purpose.

5.2.3.4 Expert 4

Expert 4 works as a Digital Forensic Analyst with only 9 months of experience. Expert 4 comments are analysed in Figure 5.11.

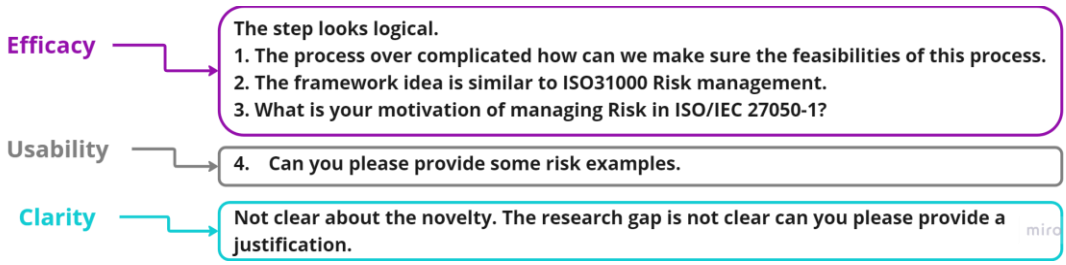


Figure 5.11: Expert 4 Comments Analysis

Despite the Expert's limited experience, the researcher sought additional feedback from a digital forensic standpoint. As outlined in Figure 5.12, Expert 4 provided 'Good' feedback regarding the possibility to align the proposed artefact with the international standards (value = 1). However, Expert 4 felt that the usefulness, usability, and possibility to improve the proposed artefact is less likely (value = -1). Expert 4 gave an 'Ok' score regarding the efficacy and clarity of the proposed artefact, as well as its potential to improve risk management (value = 0).

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
0	0	-1	1	-1	0	-1	-1

Figure 5.12: Evaluation Criteria Scores Provided by Expert 4

Expert 4 commented that the steps described in the proposed artefact look logical. However, the process is over complicated due to the unclear feasibility of this process. The proposed artefact idea is like the ISO/IEC 31000 risk management. There is no clear motivation for managing risks in ISO/IEC 27050-1. The research gap is not clear (i.e., novelty is unclear).

The overall scoring of Expert 4 feedback was approximately **- 0.4 (negative)** which sets between 0 and -1 (negative). That means the proposed artefact is 'Poor' in

terms of its quality and required key modifications made to its shape, so the improved version could be fit for purpose.

5.2.3.5 Expert 5

Expert 5 is an Academic Member of Staff working in a public university. Expert 5 has 10 years of experience in teaching Security and Risk Management subjects to a wide range of students, including undergraduates and postgraduates. Expert 5 comments are analysed in Figure 5.13.

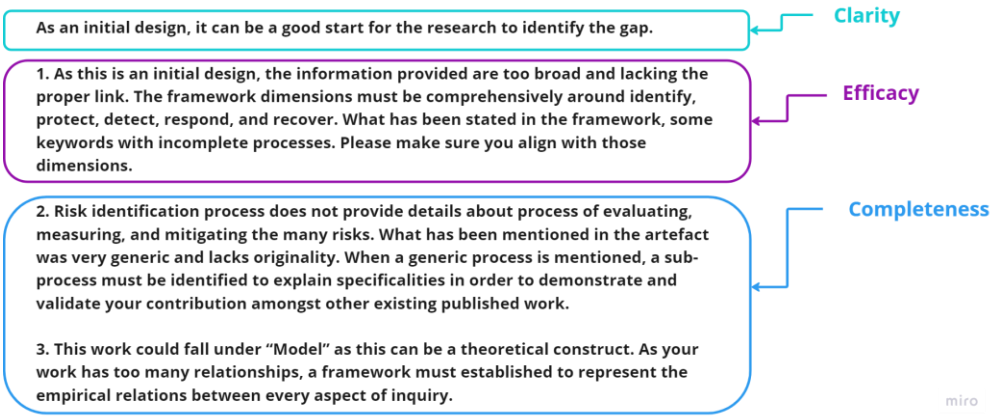


Figure 5.13: Expert 5 Comments Analysis

As outlined in Figure 5.14, Expert 5 felt that the proposed artefact is 'Ok' in terms of its efficacy, usefulness, usability, and possibility to improve risk management (value = 0) whereas it is 'Good' for its both clarity and alignment with the international standard (value = 1). However, Expert 5 believed that the proposed artefact cannot be improved at this stage as it needs major changes to enhance its quality and usability (value = -2).

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
0	1	0	1	0	0	-2	-2

Figure 5.14: Evaluation Criteria Scores Provided by Expert 5

Furthermore, Expert 5 provided three general comments below:

- As an initial design, the proposed artefact can be a good start for the research into the identified gap. The information provided is too broad and lacks the proper link. The framework dimensions must be comprehensively around identifying, protecting, detecting, responding, and recovering. There are some keywords with

incomplete processes.

- The Risk Identification Phase does not provide details about the process of evaluating, measuring, and mitigating many risks. This artefact was very generic and lacked originality. When a generic process is mentioned, a sub-process must be identified to explain specificities to demonstrate and validate the researcher's contribution amongst other existing published work.
- The proposed artefact could fall under "Model" as this can be a theoretical construct. As this work has too many relationships, a framework must be established to represent the empirical relations between every aspect of inquiry.

The overall scoring of Expert 5 feedback was approximately **- 0.3 (negative)** which sets between 0 and -1 (negative). This is because the proposed artefact seems to be more a 'Model' than a 'Framework' due to a lack of explaining the sub-components (i.e., especially from an evaluation, measuring, and mitigating perspective) and missing the relationship visibility between various components.

5.2.3.6 Expert 6

Expert 6 is a professional with 12 years of experience. Expert 6 comments are analysed in Figure 5.15.

As shown in Figure 5.16, Expert 6 did not evaluate the proposed artefact in terms of its improvability and completeness. Expert 6 comments are analysed in Figure 5.15.

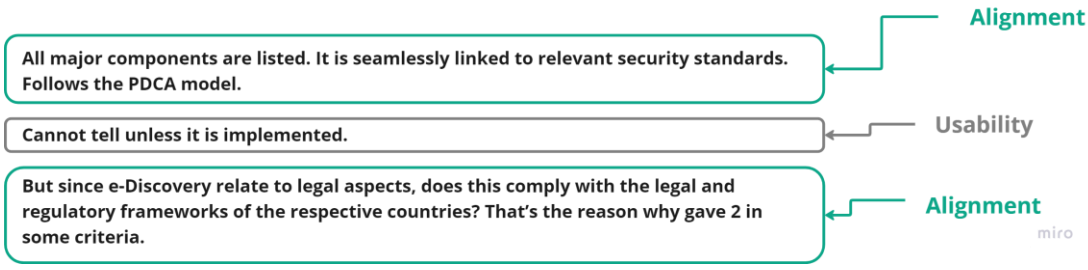


Figure 5.15: Expert 6 Comments Analysis

Expert 6 thought that the proposed artefact could be suitable for eDiscovery risk management, and clear and useful in experts' workplaces (value = 1). Expert 6 strongly believed that the proposed artefact is aligned with international security risk management and will improve the risk management framework (value = 2).

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
1	1	1	2	1	2	FALSE	FALSE

Figure 5.16: Evaluation Criteria Scores Provided by Expert 6

Expert 6 commented that all major components of the proposed artefact are listed. In addition to that, it is seamlessly linked to relevant security standards and followed the PDCA model. However, Expert 6 criticised that the weaknesses of the proposed artefact cannot be identified unless it is implemented. The overall scoring of Expert 6 feedback was approximately **1.33 (positive)** which sets between 1 and 2 (positive). This means that the proposed artefact scored "Good". Therefore, a minor change would improve its quality.

5.2.3.7 Expert 7

Expert 7 is a Cyber Security Consultant and Risk Management Practitioner with more than 10 years of experience. Expert 7 comments are analysed in Figure 5.17.

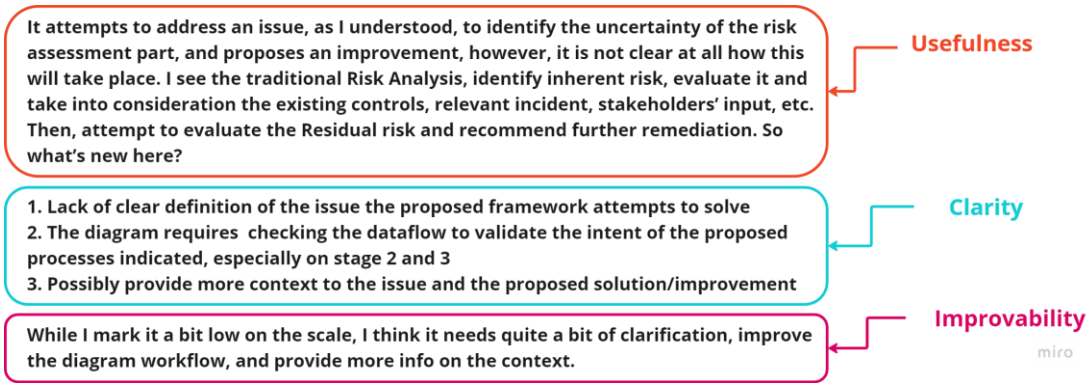


Figure 5.17: Expert 7 Comments Analysis

As can be seen in Figure 5.18, Expert 7 believed that the proposed artefact suffered from some weaknesses that affect its efficacy, clarity, usefulness, alignment with international standards, and robustness (value = -1).

Although Expert 7 gave 'Ok' to the completeness of the proposed artefact (value = 0), Expert 7 indicated that the proposed artefact cannot be used in its current state and requires major changes (value = -2). Expert 7 did not provide any feedback regarding the possibility of improving the proposed artefact.

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
-1	-1	-1	-1	-2	-1	N/A	0

Figure 5.18: Evaluation Criteria Scores Provided by Expert 7

Expert 7 commented that the proposed artefact attempts to address an issue to identify the uncertainty of the risk assessment part, and proposes an improvement, however, it is not clear at all how this will take place. It is obvious that the proposed artefact follows the traditional risk analysis that identifies inherent risk and evaluates it; and then takes into consideration the existing controls, relevant incidents, stakeholders' input, etc. Later, it attempts to evaluate the residual risk and recommend further remediation. Hence, there was no novelty.

Expert 7 reported some key weaknesses of the proposed artefact, including the lack of a clear definition of the issue the proposed artefact attempts to solve. Additionally, the proposed artefact diagram (depicted in Figure 4.28) requires checking the data flow to validate the intent of the proposed processes indicated, especially in the Risk Identification and Risk Estimation phase. Lastly, the researcher possibly needs to provide more context to the issue and the proposed solution/improvement.

On the other hand, while Expert 7 marked the proposed artefact Low on the scale, Expert 7 thought it needs quite a bit of clarification, improve the diagram workflow, and provide more information on the context. The overall scoring of Expert 7 feedback was approximately **-1 (negative)**. That means the proposed artefact is 'Poor' in terms of its quality and required key modifications made to its shape, so the improved version could be fit for purpose.

5.2.3.8 Expert 8

Expert 8 is an Information Security Consultant with 22 years of experience. Expert 8 comments are analysed in Figure 5.19.

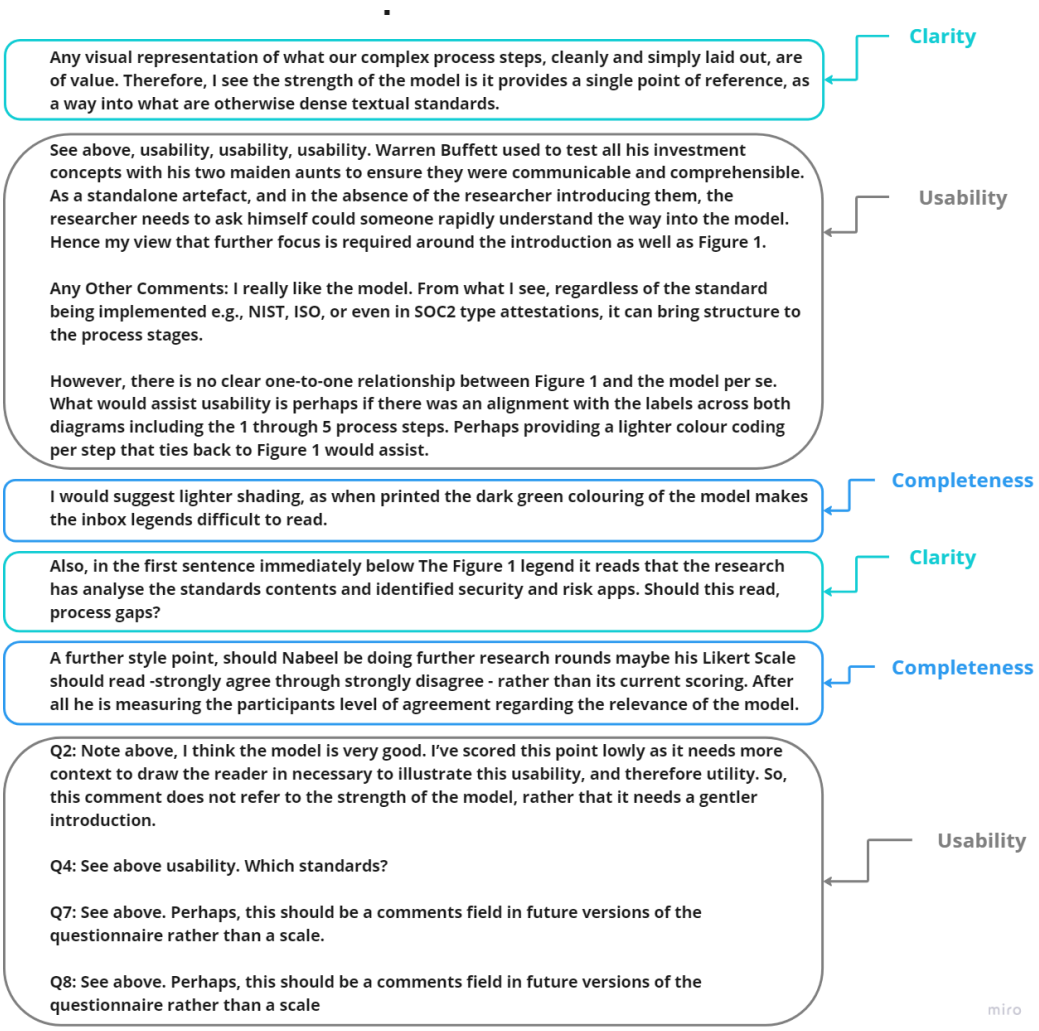


Figure 5.19: Expert 8 Comments Analysis

As outlined in Figure 5.20, Expert 8 provided various scores for the proposed artefact quality. Expert 8 thought that the proposed artefact has a 'Good' score in terms of its efficacy, usefulness, and robustness (value = 1).

The possibility to align the proposed artefact with international standards is neutral (value = 0). This also applies to the chance of improving the proposed artefact in its current state (value = 0). Expert 8 responded 'Ok' to the required modifications to be made to any component of the proposed artefact (value = 0). On the other hand, Expert 8 observed that the defined components of the proposed artefact are not clear (value = -1).

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
1	-1	1	0	2	1	0	0

Figure 5.20: Evaluation Criteria Scores Provided by Expert 8

Expert 8 commented that any visual representation of complex process steps, cleanly, and simply laid out, is of value. Therefore, Expert 8 saw the strength of the model as it provides a single point of reference, as a way into what are otherwise dense textual standards.

However, from a weaknesses and improvements perceptive, Expert 8 commented that as a standalone artefact, and in the absence of the researcher introducing them, it is important to ask, could someone rapidly understand the way into the model? Hence, Expert 8 view was that further focus is required around the introduction as well as the eDiscovery process phases (depicted in Figure 2.8). Expert 8 emphasised that the usability of the proposed artefact is paramount.

In general, Expert 8 commented that from what it was observed, regardless of the standard being implemented (e.g., NIST, ISO, or even in SOC 2 type 2 attestations), the proposed artefact can bring structure to the process stages. However, there is no clear one-to-one relationship between the eDiscovery process phases (depicted in Figure 2.8) and the proposed artefact in itself. What would assist usability is perhaps if there was an alignment with the labels across both diagrams (i.e., the proposed artefact illustrated in Figure 4.28 and the eDiscovery process phases shown in Figure 2.8) including the 1 through 5 process steps. Perhaps providing a lighter colour coding per step that ties back to each step would assist. Expert 8 suggested that lighter shading, as when printed the dark green colouring of the model makes the inbox legends difficult to read. Additionally, in the first sentence immediately below the Figure 2.8 legend, it reads that the research has analysed the contents of the standard and identified security and risk applications. Should this read, process gaps?

Expert 8 believed that the proposed artefact was very good. Expert 8 scored the usability of the proposed artefact Low as it needs more context to draw the reader in and to illustrate this usability, and therefore utility. Expert 8 commented that this comment (around usability) does not refer to the strength of the proposed artefact, but rather that it needs a gentler introduction.

The overall scoring of Expert 8 feedback was approximately 0.5 (positive) which sets between 0 and 1 (positive). This means that the proposed artefact requires more attention to its usability as explained above.

5.2.3.9 Expert 9

Expert 9 has more than 7 years of experience and works as an Information Security Manager. Expert 9 comments are analysed in Figure 5.21.

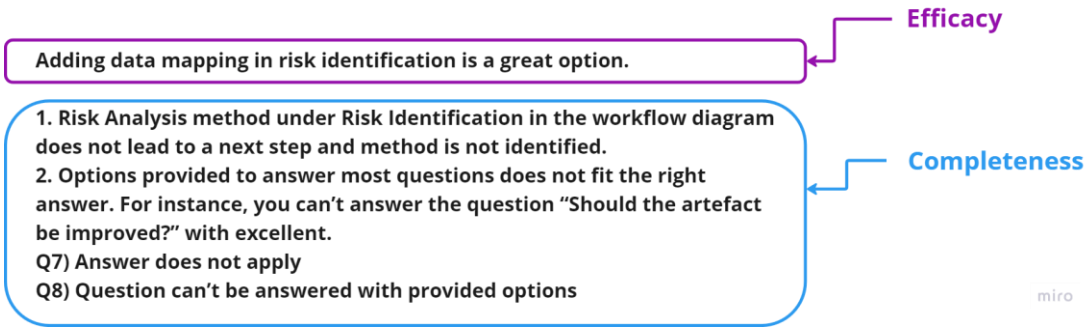


Figure 5.21: Expert 9 Comments Analysis

As shown in Figure 5.22, Expert 9 has agreed that the proposed artefact would be effective for eDiscovery risk management as well as it could be aligned with the international standards (value = 2). Moreover, Expert 9 felt that 'Good' is the right score given to the proposed artefact in terms of its efficacy, usefulness, and usability (value = 1).

Expert 9 neither agreed nor disagreed about the robustness of the proposed artefact (value = 0). Expert 9 did have an opinion about if the proposed artefact would be improved, and if positive, then what are modifications required.

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
1	2	1	2	1	0	N/A	N/A

Figure 5.22: Evaluation Criteria Scores Provided by Expert 9

Expert 9 indicated that adding the "Data Mapping" activity in the Risk Identification phase was a great option. On the other hand, Expert 9 commented that the "Risk Analysis" method under the Risk Identification phase in the workflow diagram does not lead to a next step and the method is not identified. This comment was provided as one of the key weaknesses of the proposed artefact.

The overall scoring of Expert 9 feedback was approximately 1.2 (positive) which sets between 1 and 2 (positive). This means that the proposed artefact scored "Good". Hence, a minor change would improve its quality.

5.2.3.10 Expert 10

Expert 10 works as a Cyber Security Manager with 21 years of experience. Expert 10 comments are analysed in Figure 5.23.

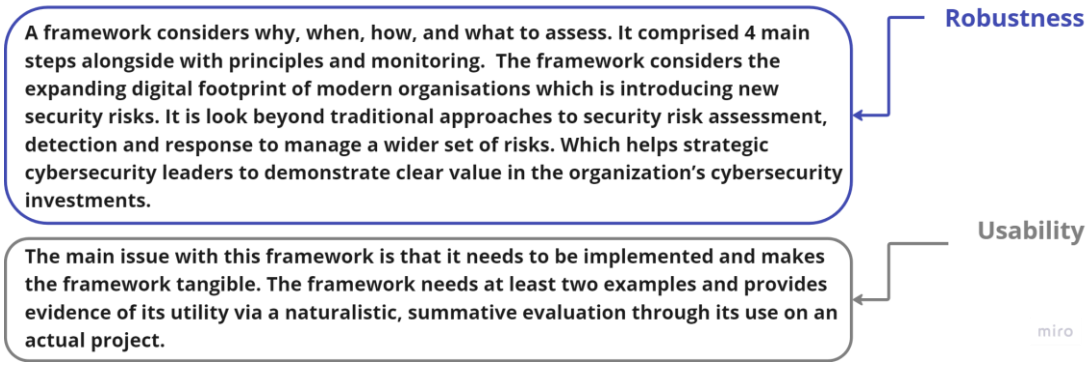


Figure 5.23: Expert 10 Comments Analysis

As outlined in Figure 5.24, Expert 10 indicated that the proposed artefact is 'Poor' in terms of its efficacy and alignment with the international standards (value = -1). In addition to that, Expert 10 thought that the proposed artefact would not be able to improve risk management at this stage and needs to be enhanced from its structure perceptive (value = -1).

On the other hand, Expert 10 gave an 'Ok' score to its components' clarity, usefulness, usability, and complements (value = 0).

Evaluation Criteria							
Efficacy	Clarity	Usefulness	Alignment	Usability	Robustness	Improvability	Completeness
-1	0	0	-1	0	-1	-1	0

Figure 5.24: Evaluation Criteria Scores Provided by Expert 10

Expert 10 believed that the proposed framework has considered why, when, how, and what to assess. It comprised four main steps alongside principles and monitoring. It considered the expanding digital footprint of modern organisations towards introducing new security risks. It looked beyond traditional approaches to security risk assessment, detection, and response to manage a wider set of risks. This capability would help strategic cybersecurity leaders to demonstrate a clear value in the organisations' cybersecurity investments. However, Expert 10 stated that the main issue with this

framework is that it needs to be implemented and make the framework tangible. The framework needs at least two examples and provides evidence of its utility via a naturalistic and summative evaluation through its use on an actual project.

The overall scoring of Expert 10 feedback was approximately **-0.5 (negative)** which sets between 0 and -1 (negative). This means that the proposed artefact needs some modifications to improve its quality through proven use cases.

Expert feedback to the provided set of questions is recorded in Table A4.1 to Table A4.10 in Appendix A4.

5.2.4 Critical Reflection on Experts' Evaluation Results

Experts' artefact evaluation is an essential phase in the researcher's selection of methods (i.e., ADSRM approach) described previously in Section 3.4. This essential phase is beneficial due to its outcomes that represent the authentic and current feedback of the proposed artefact. Moreover, it aids the researcher in obtaining valuable insights and knowledge during the collection and analysis of experts' opinions. By scrutinising and assessing the proposed artefact and the researcher, this phase facilitates valuable feedback and enhances the research process.

The Experts' evaluations have been reviewed for critical analysis, assessed, and populated with the researcher's comments as explained in the next subsections.

5.2.4.1 Efficacy for Electronic Discovery Risk Management

Q1) Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?

Expert 1, Expert 2, Expert 4, and Expert 8 believed that the proposed artefact is very good, solid, logical, and clear. However, it has been reported by Expert 5 that the proposed artefact does not cover the five dimensions of a full security framework: identify, protect, detect, respond, and recover. The researcher argues that the key objective of the proposed artefact is to have a ready reference model to guide information security actions at each process step of the ISO/IEC 27050 for the ESI process. This includes identification, preservation, collection, processing, review, production, and analysis. It does not necessarily need to follow the five functions of the NIST Cybersecurity Framework.

On the other hand, Expert 4 criticised that the proposed artefact has a similarity with the ISO/IEC 31000 risk management structure. This is partially a true statement because the researcher used various international standards (as explained in Section 2.4)

to build the intended artefact (i.e., the principles building block was built based on the ISO/IEC 31000). Expert 4 also added that the proposed process is over complicated due to the absence of a proper feasibility study.

The researcher responds to this criticism by emphasising that only a brief introduction was communicated to all experts for their opinion. The researcher does not intend to provide full details of this study, including a feasibility study. Instead, the experts were invited to provide their feedback to further guide and develop the researcher's thinking; and ultimately to improve the current framework.

Expert 9 commented that adding the "Data mapping" component in the Risk Identification phase is a great option. This new component was introduced during Artefact 2 as an appropriate activity that has a centralised inventory listing of what types of ESI an organisation has and where they are stored. It was also a key output when creating a DFD and BPM.

5.2.4.2 Clarity of Components

Q2) Are the defined components of the proposed artefact clear and relevant to what you observe?

Expert 2 raised a question regarding the difference between the 'Vulnerability' component listed in the Risk Identification phase and the Risk Estimation phase. The key distinction between them is that the first 'Vulnerability' component aims to identify the vulnerability while the other one focuses on determining the probability of vulnerability (i.e., the likelihood that a threat event will become a loss event). The vulnerability is calculated via two primary factors: Threat Capability and Control Strength (as explained in Section 4.1.4.5, 4.1.5.5, and 4.1.5.8 respectively).

Expert 5 criticised that this work could fall under "Model" as this can be a theoretical construct. Since this work has too many relationships, a framework must be established to represent the empirical relations between every aspect of inquiry.

Similarly, Expert 7 criticised that this study does not have a clear definition of the issue the proposed artefact attempts to solve. Expert 7 suggested that the researcher needs to provide more context to the issue and the proposed solution/improvement. The researcher does not fully agree with the Expert 5 and Expert 7 comments because the proposed framework was tested against three real scenarios (as presented in Sections 4.1, 4.2, and 4.3 respectively). The experts were given limited information to evaluate the proposed artefact without supporting it with the scenarios in question.

Expert 7 pointed out that the diagram of the proposed artefact needs to be revisited to validate the proposed dataflow process, especially in the Risk Identification phase and the Risk Estimation phase. This is a fair observation which will be articulated in the Artefact improvement stage.

Expert 8 indicated that the proposed artefact provides a single point of reference with a visual representation in contrast to other standards. This is considered one of the strongest attributes of the proposed artefact. The researcher agrees that describing the artefact components using a graphical representation can simplify the complicated process steps.

5.2.4.3 Usefulness to Workplace

Q3) How useful is the proposed artefact for your workplace?

Expert 7 believed that the proposed artefact does not provide any novelty and does not add any value. This is because it follows a traditional risk analysis process by identifying inherent risk, evaluating it, and taking into consideration the existing controls, relevant incidents, and stakeholders' input. Then, it evaluates the residual risk and recommends further remediation. The researcher argues that the proposed artefact brings novelty by adding value to the recently released standards and guidelines for eDiscovery by providing a risk evaluation framework for users. At present, the eDiscovery guidelines ignore security risks and are populated by technical assistance for discovery. The use of these guidelines without a risk evaluation framework puts the users and the information at risk of disclosure and damage. The intention was to design an effective risk evaluation framework and then to scenario test it for efficiency.

5.2.4.4 Alignment with International Security Risk Management Standards

Q4) Does the proposed artefact align with the international security risk management standards?

Expert 2 and Expert 6 believed that the proposed artefact would be useable depending on the level of end-user understanding. This is because of several reasons the proposed artefact is aligned with ISO standards, it consists of all major components, it is seamlessly linked to relevant security standards, and it follows the Plan-Do-Check-Act (PDCA) model. This is true as the proposed artefact intended to evaluate risks in the eDiscovery context. As mentioned previously, the proposed artefact is aligned with

numerous standards, including ISO/IEC 31000, ISO/IEC 27005, and NIST Risk Management Framework.

On the other hand, Expert 6 raised an interesting question that is: since eDiscovery relates to legal aspects, does the proposed artefact comply with the legal and regulatory frameworks of the respective countries? To answer this question, it is important to emphasise that the proposed artefact is aligned with the international standards as explained previously and does not have specific requirements to any legal or regulatory requirements. The assessor who wants to evaluate eDiscovery security risk needs to identify business requirements and any relevant legal and regulatory requirements during the Context Establishment phase. Identifying legal and regulatory requirements for respective countries will rely on the scope of the assessment and the location of ESI. Hence, the researcher has only analysed and conducted a comparative review of numerous information security risk analysis methodologies (refer to Section 2.4).

5.2.4.5 Usability and Implementation

Q5) Is it usable?

Expert 4 believed that this study does not provide any risk examples which led to not fully understanding the proposed artefact usability and implementation. Furthermore, Expert 10 commented that the proposed artefact needs at least two examples and provides evidence of its utility via a naturalistic and summative evaluation through its use on an actual project. As addressed previously, the researcher did not share the full details of the proposed artefact, including process description, assumptions, and testing scenarios with risk examples. This is because the intention was to provide the experts with a brief description of the proposed artefact, including the problem statements, rationale, and a high-level process diagram.

Expert 6 reported that usability cannot be evaluated unless the proposed artefact is implemented. Similarly, Expert 10 criticised that the main issue with the proposed artefact is that it needs to be implemented to make it tangible. Although implementation is a necessary step that transforms the plan into action to achieve the defined goals, it was considered as part of this research. The reason behind that is that the proposed artefact mainly focuses on testing scenarios and expert evaluation.

Expert 8 liked the model and believed that regardless of the standard being implemented (e.g., NIST, ISO, or even in SOC2 type 2 attestations), it can bring structure

to the process stages. However, Expert 8 found that there is no clear one-to-one relationship between the diagram of the proposed artefact and the model itself.

Expert 8 assumed that the usability of the proposed artefact could be enhanced if there was an alignment with the labels across both the proposed artefact diagram and the eDiscovery process diagram including the 1 through 5 process steps. Perhaps providing a lighter colour coding per step that ties back to the proposed artefact diagram would assist. The researcher admits that the alignment between the proposed artefact and the eDiscovery process was not clear. This would be a great adjustment to be made to the proposed artefact to improve the overall framework usability.

5.2.4.6 Robustness for Risk Management Improvement

Q6) Will it improve risk management?

Expert 10 provided an overall observation about this study. Expert 10 stated that the proposed framework considers why, when, how, and what to assess. It comprised four main steps alongside principles and monitoring. Furthermore, the framework considers the expanding digital footprint of modern organisations which is introducing new security risks. It looks beyond traditional approaches to security risk assessment, detection, and responses to manage a wider set of risks. This would help strategic cybersecurity leaders to demonstrate tangible value in the organisation's cybersecurity investments. The researcher thinks the statements above summarise the key objectives of the proposed artefact and highlights the key differentiator between the current frameworks and the proposed one.

5.2.4.7 Improvability of the Artefact

Q7) Should the artefact be improved?

Expert 7 thinks that the proposed artefact needs quite a bit of clarification, to improve its diagram workflow, and provide more information on the context. On the other hand, Expert 1 commented that as an improvement the researcher needs to consider adding a feedback loop from the Risk Treatment phase back to the Risk Level component. This is to re-assess the risk level after being treated. The researcher believes that the suggestions above will be considered as part of the overall improvement (i.e., listed in Section 5.3.4 and detailed in Section 5.4).

5.2.4.8 Completeness and Modifications

Q8) Should modifications be made to any component of the proposed artefact?

Expert 2 reported that the ‘Metric Determination’ is a missing component in the Monitoring & Improvement phase. Moreover, Expert 2 added that as part of the Risk Monitoring process, the researcher should define the objectives of this process to set out what is to be monitored, how it is measured, who does it, and when and how it is sourced and evidenced. The researcher agrees that risk metrics are an important component to measure the effectiveness of overall risk management. This could be considered in the updated version of the proposed artefact. Nevertheless, the researcher will take into consideration the above-suggested objectives of the monitoring to reshape the Risk Monitoring process of the proposed artefact.

Expert 2 suggested adding a ‘Method Selection’ component as part of the Risk Monitoring & Improvement phase to produce comparable and reproducible results. Additionally, the introduction of a new component for regular ‘Internal Audits’ provides a determination of nonconformity / corrective action/improvement. The researcher believes that the audit activity is out of scope as the main objective of the proposed artefact is to identify and assess potential security risks in the eDiscovery context.

Expert 3 commented that every risk has its situation, therefore it is better to focus on a wide risk management framework and better to add risk mitigation components as well. The researcher has already included a ‘Risk Treatment Plan’ component as part of the Risk Evaluation & Treatment phase. The proposed artefact was developed as a complete risk management framework with sub-processes to fulfil its objectives.

Expert 5 criticised that the Risk identification process does not provide details about the process of evaluating, measuring, and mitigating various risks. What has been mentioned in the artefact was very generic and lacks originality. When a generic process is mentioned, a sub-process must be identified to explain specificities to demonstrate and validate the researcher’s contribution amongst other existing published work. As the researcher explained previously, the experts were given a brief description of the proposed artefact with a graphical presentation of a workflow (i.e., phases and components/activities). The researcher has conducted a literature review to identify the actual research gaps and then proposed a new solution (refer to Section 2.3 and 2.7 respectively).

5.2.5 Recording Results

Figure 5.25 records the results of the feedback in which 10 experts were asked to provide their opinion regarding eight key features of the proposed artefact: efficacy, clarity,

usefulness, alignment, usability, robustness, improvability, and completeness respectively. The opinions were extracted and analysed from the data collected during the experts' feedback process. This provides different perspectives and points of view that help improve the proposed Artefact 2 and validation.

The stacked bar chart in Figure 5.25 shows the 5-point Likert results. Each bar shows the total percentage of each evaluation criterion distributed among the 5-point scale. From the stacked bar chart, it is clear that the majority of the experts believe that the proposed artefact would be effective for eDiscovery risk management (i.e., efficacy), with just 20% thinking it needs some modifications to be made to its components. For example, Expert 5 reported that the proposed artefact has too many relationships and could fall under "Model" as this can be a theoretical construct. A framework must be established to represent the empirical relations between every aspect of inquiry.

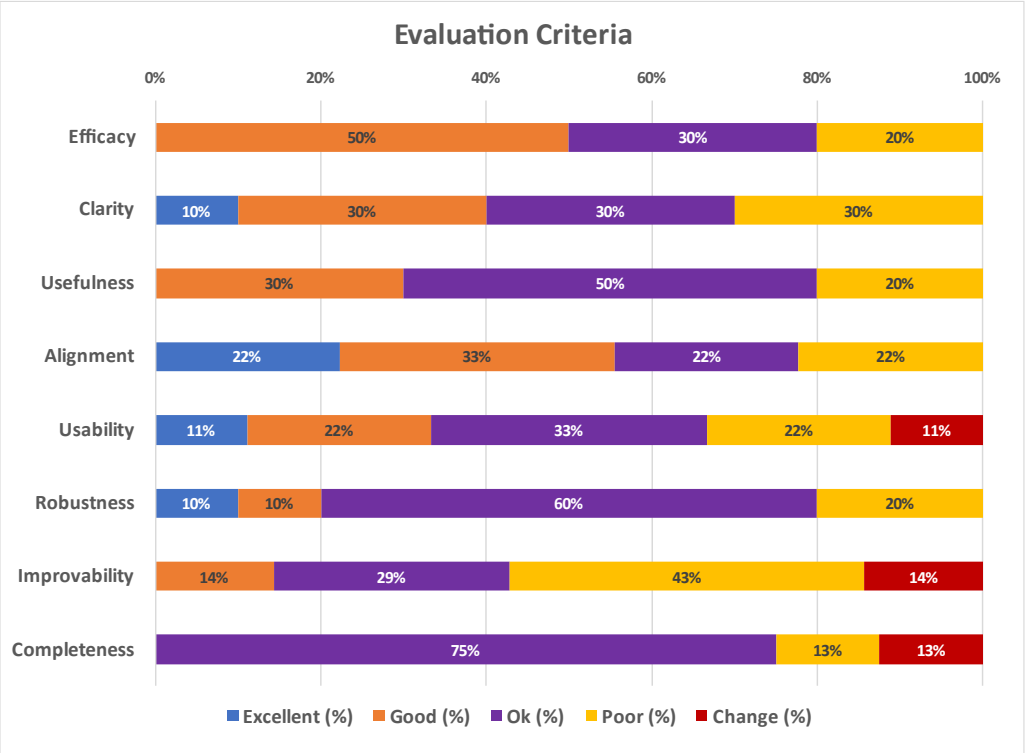


Figure 5.25: Evaluation Criteria Results Provided by Experts

Nearly two-thirds of the experts observe that the defined components of the proposed artefact are clear and relevant (i.e., clarity). The other third believes that they are not, and a small minority (10%) thinks its components are 'Excellent' for clarity. For example, there is no clear distinction between the 'Vulnerability" component listed in both the Risk Identification phase and the Risk Estimation phase (addressed by Expert 2).

Most of the experts indicate that the proposed artefact would be useful for their workplace (usefulness), while only 20% believe that it cannot be useful in its current state. Thus, it has been noted by both Expert 6 and Expert 10 that the weaknesses of the proposed artefact cannot be identified unless it is implemented, and thus this will make the framework tangible, demonstrable, and verifiable.

Similarly, around 80% of the experts think that the proposed artefact is aligned with the international security risk management standards (i.e., alignment) whereas approximately 20% say it cannot be aligned in its present state.

When the experts responded to the proposed artefact's usability, two-thirds of them acknowledge that it could be useable at its current state (i.e., usability) but the rest of them disagree. For instance, Expert 8 observes that there is no clear one-to-one relationship between the eDiscovery process phases and the proposed artefact. On the other hand, 80% of the experts believe that the proposed artefact will improve risk management (i.e., robustness).

Furthermore, less than 50% of the expert feedback says that the proposed artefact should be enhanced (i.e., improvability). To achieve the desired enhancement, 75% of the experts believe that some adjustments/corrections should be enacted to specific components of the proposed artefact (completeness). For instance, the recommended changes would be placing loop feedback between the Risk Estimation phase and the Risk Evaluation & Treatment phase (suggested by Expert 1) as well as adding Risk Mitigation components as part of the Risk Evaluation & Treatment phase (recommended by Expert 3).

5.3 ARTEFACT THEMATIC EVALUATION

Thematic evaluation, a widely employed approach in qualitative research, involves a subjective qualitative investigation to address various research questions. It is mainly used by many researchers to conduct a qualitative research analysis, as it offers great flexibility that can be tailored to the specific study's needs. The key benefit of using a thematic analysis is its ability to explore the viewpoints of different research participants, uncovering both commonalities and differences and then generating unexpected insights. Additionally, it serves as a valuable tool for summarising key attributes of large data sets, allowing researchers to employ a well-structured approach in handling the data, and ultimately leading to clear and organised final results (Nowell et al., 2017). In this

research, a thematic evaluation has been conducted for the data gathered from the experts using the NVivo tool as explained in the subsections below.

5.3.1 Preparing Dataset

A dataset contains structured data arranged in rows and columns. The dataset is created by importing data into NVivo and cannot be edited. In this research, the dataset contains expert feedback. Their feedback was set it up in text documents before being imported into NVivo. The feedback was received in Microsoft Word format (i.e., each expert filled up a separate file). Then, a separate Microsoft Excel spreadsheet format was created (i.e., that consolidates all feedback in a single file) specifically for importing into NVivo as illustrated in Figure 5.26 with the following structure:

- The questions are in the column headings in row 1. This is to ensure that they will appear in the Nvivo interface in a certain order.
- Only the first row contains columns or field names with ID, Expert Name, Question 1, Question 2, etc.
- Each column contains a unique identifier (i.e., an ID number for each expert, Expert 01, Expert 02, etc.

After importing the dataset, various queries and procedures were applied to perform the thematic investigation using the NVivo tool.

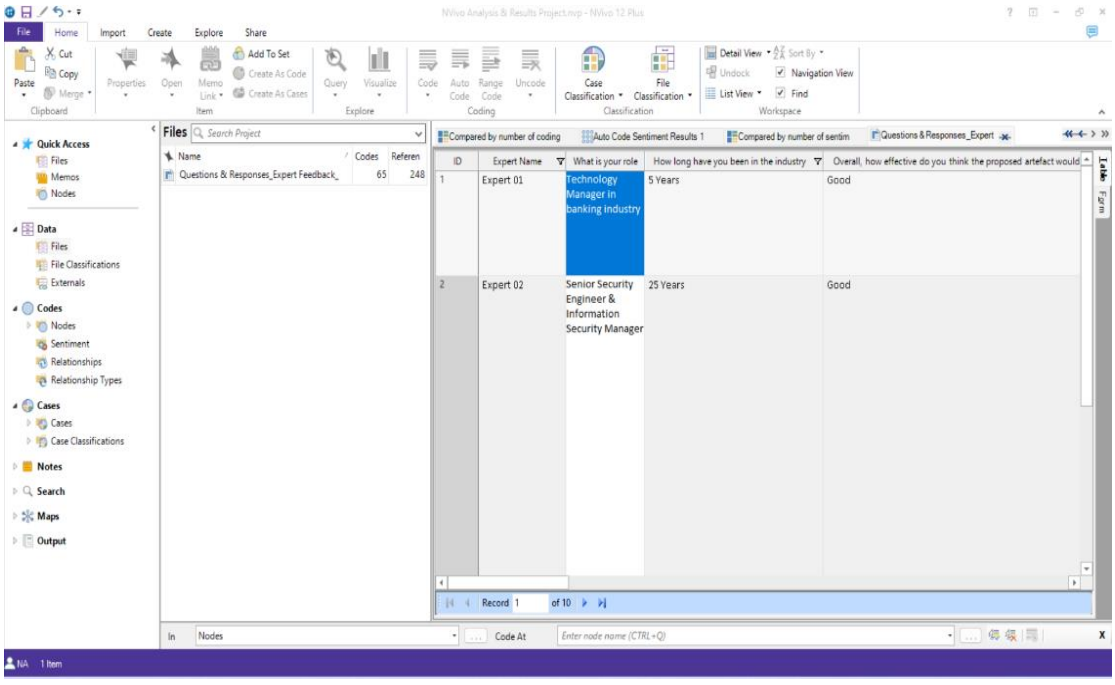


Figure 5.26: Dataset Imported into NVivo Tool

5.3.2 Word Frequency Analysis Result

The NVivo tool includes a functionality called word frequency queries, which provides a list of the most commonly used words or ideas found in a specific source. This can help the researcher to identify possible themes and analyse the most frequently used words in a particular demographic. The default setting of word frequency criteria is the top 1,000 words with a minimum of 4 characters. The referenced source is stored in a Microsoft Excel format containing feedback text from the selected experts. Figure 5.27 shows the 100 most frequent words used in the expert feedback.

Figure 5.27: The Top 100 Frequent Words (Word Cloud)

For the next analysis, the researcher has set the criteria to the top 20 frequent words with a minimum of 3 characters as presented in Table 5.3 and illustrated in Figure 5.28.

Table 5.3: The Top 20 Frequent Words Summary

Rank	Word	Count	Weighted	Rank	Word	Count	Weighted
1	Risk	23	2.77%	11	Clear	7	0.72%
2	Good	20	2.41%	12	Comments	6	0.72%
3	Poor	17	1.33%	13	Excellent	6	0.72%
4	Framework	11	1.33%	14	Needs	6	0.72%
5	Process	11	1.20%	15	Usability	6	0.60%
6	Expert	10	1.20%	16	Improvement	5	0.60%
7	Model	10	1.20%	17	Perhaps	5	0.60%
8	Years	10	1.08%	18	Provide	5	0.60%
9	Security	9	1.08%	19	Answer	4	0.48%
10	See	9	0.84%	20	Figure	4	0.48%

Figure 5.28: The Top 20 Frequent Words (Word Cloud)

NVivo provides a flexible way to run a Text Search query beyond extract matches to find similar words such as synonyms. NVivo can group similar words, allowing researchers to easily identify the most frequently occurring words. There are five levels/groups as described in Table 5.4. All these five levels/groups were considered for examining word frequency in this evaluation.

Table 5.4: Text Marching Levels / Grouping Description in NVivo Tool

Level / Grouping	Name	Returns	Example (Process)
1	Exact Matches	▪ Exact matches only (default)	process
2	Stemmed Words	▪ Exact matches ▪ Words with the same stem	process, processes
3	Synonymous Words	▪ Exact matches ▪ Words with the same stem ▪ Synonyms (words with a very close meaning)	process, processes, action, treated, work
4	Specialisation	▪ Exact matches ▪ Words with the same stem ▪ Synonyms (words with a very close meaning) ▪ Specialisations (words with a more specialised meaning)	process, processes, action, treated, work, analysis, issue, solve
5	Generalisation	▪ Exact matches ▪ Words with the same stem ▪ Synonyms (words with a very close meaning)	process, processes, action, treated, work, analysis, issue,

Level / Grouping	Name	Returns	Example (Process)
		▪ Specializations (words with a more specialised meaning - a type of) ▪ Generalisations (words with a more general meaning)	solve, reference, part

Figure 5.29, Figure 5.30, and Figure 5.31 illustrate the outcomes of the top 10 most frequent words from the three first levels of query: exact matching, stemmed words, and synonyms words respectively.

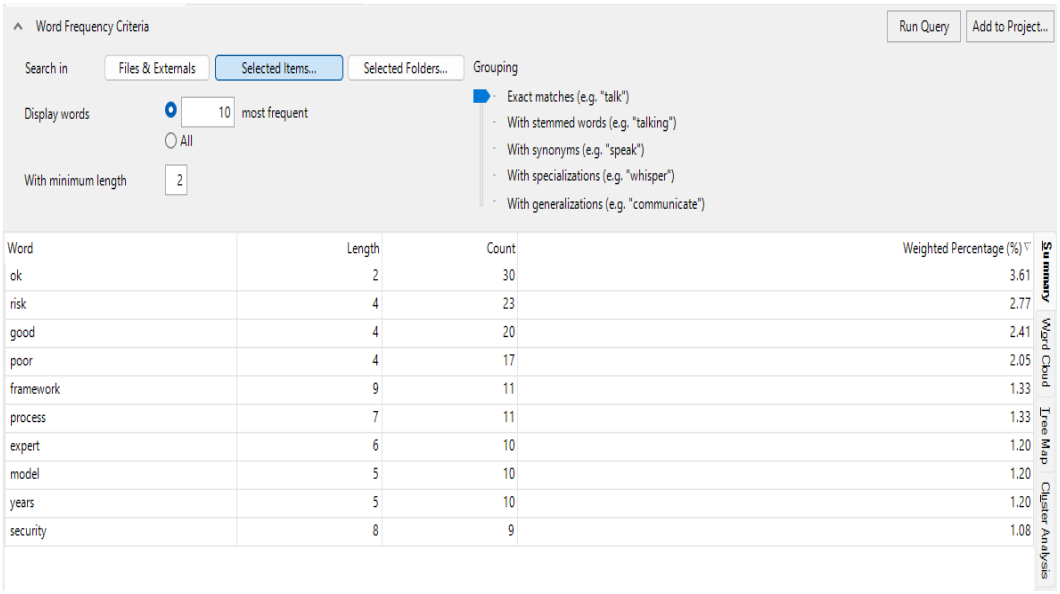
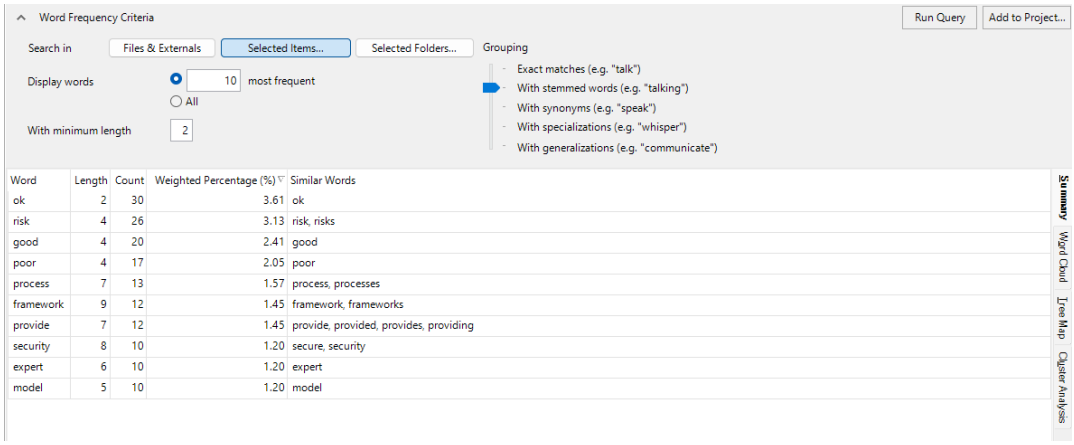
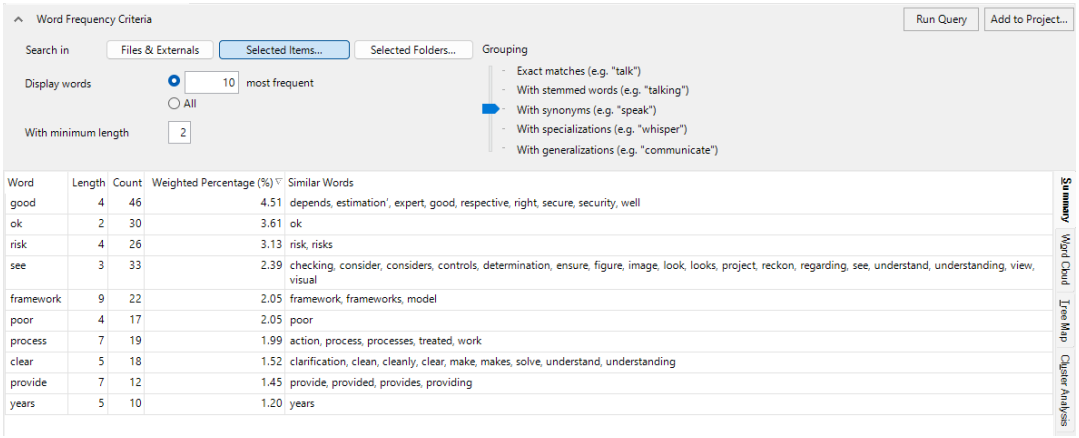


Figure 5.29: Exact Matching of Top 10 Most Frequent Words (Level 1)



Word	Length	Count	Weighted Percentage (%)	Similar Words
ok	2	30	3.61	ok
risk	4	26	3.13	risk, risks
good	4	20	2.41	good
poor	4	17	2.05	poor
process	7	13	1.57	process, processes
framework	9	12	1.45	framework, frameworks
provide	7	12	1.45	provide, provided, provides, providing
security	8	10	1.20	secure, security
expert	6	10	1.20	expert
model	5	10	1.20	model

Figure 5.30: Stemmed Matching of Top 10 Most Frequent Words (Level 2)

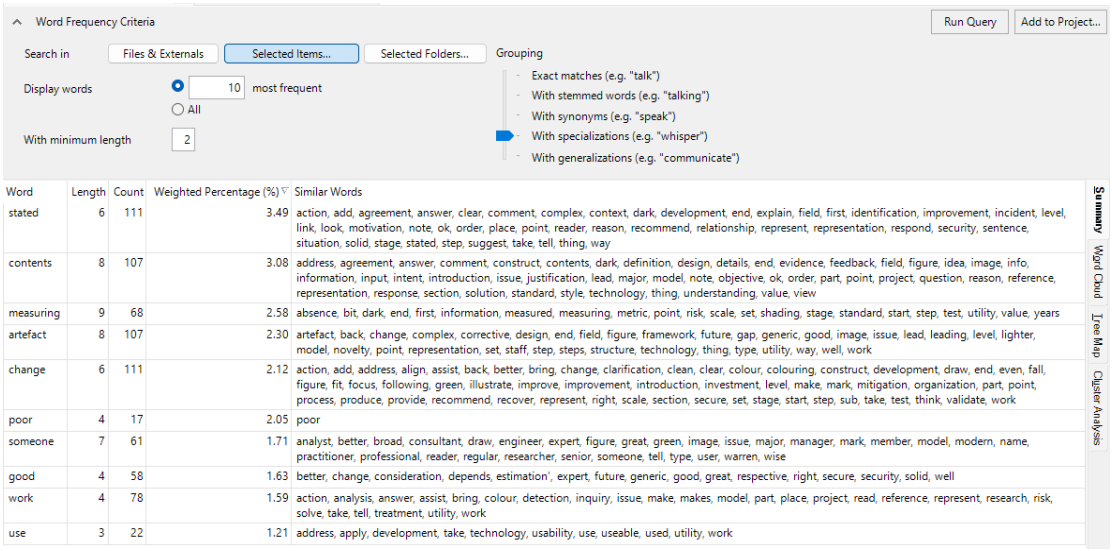


Word	Length	Count	Weighted Percentage (%)	Similar Words
good	4	46	4.51	depends, estimation', expert, good, respective, right, secure, security, well
ok	2	30	3.61	ok
risk	4	26	3.13	risk, risks
see	3	33	2.39	checking, consider, considers, controls, determination, ensure, figure, image, look, looks, project, reckon, regarding, see, understand, understanding, view, visual
framework	9	22	2.05	framework, frameworks, model
poor	4	17	2.05	poor
process	7	19	1.99	action, process, processes, treated, work
clear	5	18	1.52	clarification, clean, cleanly, clear, make, makes, solve, understand, understanding
provide	7	12	1.45	provide, provided, provides, providing
years	5	10	1.20	years

Figure 5.31: Synonyms of Top 10 Most Frequent Words (Level 3)

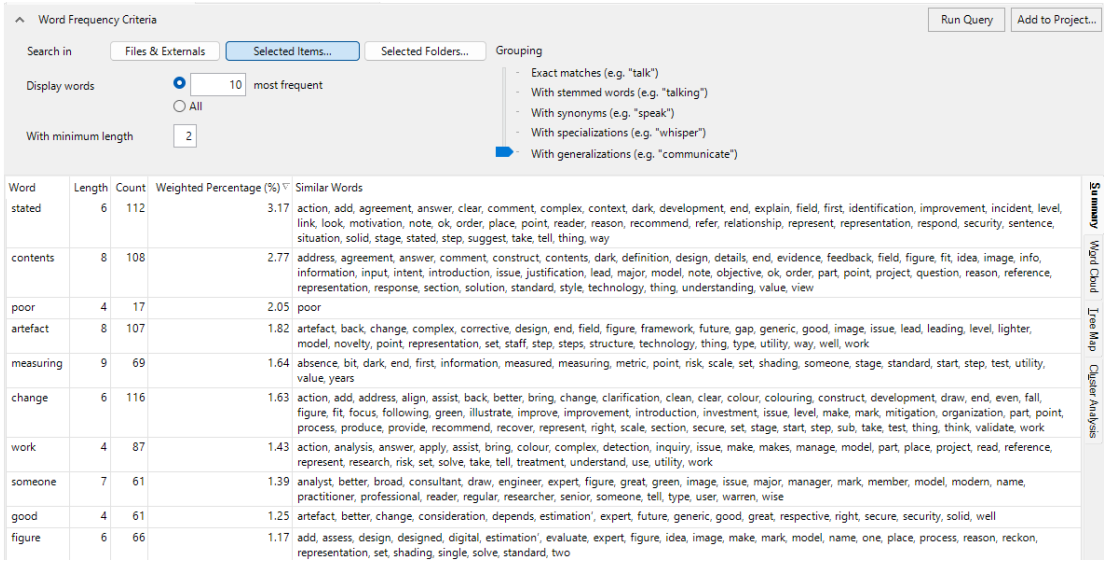
Figure 5.32 and Figure 5.33 illustrate the outcomes of the top 10 most frequent words from the other two levels of query: specialisation and generalisation respectively.

It has been recorded that the word “measuring” and its similar words appeared 68 times and 69 times in both level 4 (specialisation) and level 5 (generalisation). This demonstrates that the experts suggested improving the proposed artefact by amending a measurement phase to the proposed artefact (i.e., see the words “absence”, “metrics”, and “measured”). Likewise, the experts encourage the researcher to enact changes to the artefact components to improve its overall quality.



Word	Length	Count	Weighted Percentage (%)	Similar Words
stated	6	111	3.49	action, add, agreement, answer, clear, comment, complex, context, dark, development, end, explain, field, first, identification, improvement, incident, level, link, look, motivation, note, ok, order, place, point, reader, reason, recommend, relationship, represent, representation, respond, security, sentence, situation, solid, stage, stated, step, suggest, take, tell, thing, way
contents	8	107	3.08	address, agreement, answer, comment, construct, contents, dark, definition, design, details, end, evidence, feedback, field, figure, idea, image, info, information, input, intent, introduction, issue, justification, lead, major, model, note, objective, ok, order, part, point, project, question, reason, reference, representation, response, section, solution, standard, style, technology, thing, understanding, value, view
measuring	9	68	2.58	absence, bit, dark, end, first, information, measured, measuring, metric, point, risk, scale, set, shading, stage, standard, start, step, test, utility, value, years
artefact	8	107	2.30	artefact, back, change, complex, corrective, design, end, field, figure, framework, future, gap, generic, good, image, issue, lead, leading, level, lighter, model, novelty, point, representation, set, staff, step, steps, structure, technology, thing, type, utility, way, well, work
change	6	111	2.12	action, add, address, align, assist, back, better, bring, change, clarification, clean, clear, colour, colouring, construct, development, draw, end, even, fall, figure, fit, focus, following, green, illustrate, improve, improvement, introduction, investment, level, make, mark, mitigation, organization, part, point, process, produce, provide, recommend, recover, represent, right, scale, section, secure, set, stage, start, step, sub, take, test, think, validate, work
poor	4	17	2.05	poor
someone	7	61	1.71	analyst, better, broad, consultant, draw, engineer, expert, figure, great, green, image, issue, major, manager, mark, member, model, modern, name, practitioner, professional, reader, regular, researcher, senior, someone, tell, type, user, warren, wise
good	4	58	1.63	better, change, consideration, depends, estimation', expert, future, generic, good, great, respective, right, secure, security, solid, well
work	4	78	1.59	action, analysis, answer, assist, bring, colour, detection, inquiry, issue, make, makes, model, part, place, project, read, reference, represent, research, risk, solve, take, tell, treatment, utility, work
use	3	22	1.21	address, apply, development, take, technology, usability, use, useable, used, utility, work

Figure 5.32: Specialisation of Top 10 Most Frequent Words (Level 4)



Word	Length	Count	Weighted Percentage (%)	Similar Words
stated	6	112	3.17	action, add, agreement, answer, clear, comment, complex, context, dark, development, end, explain, field, first, identification, improvement, incident, level, link, look, motivation, note, ok, order, place, point, reader, reason, recommend, refer, relationship, represent, representation, respond, security, sentence, situation, solid, stage, stated, step, suggest, take, tell, thing, way
contents	8	108	2.77	address, agreement, answer, comment, construct, contents, dark, definition, design, details, end, evidence, feedback, field, figure, fit, idea, image, info, information, input, intent, introduction, issue, justification, lead, major, model, note, objective, ok, order, part, point, project, question, reason, reference, representation, response, section, solution, standard, style, technology, thing, understanding, value, view
poor	4	17	2.05	poor
artefact	8	107	1.82	artefact, back, change, complex, corrective, design, end, field, figure, framework, future, gap, generic, good, image, issue, lead, leading, level, lighter, model, novelty, point, representation, set, staff, step, steps, structure, technology, thing, type, utility, way, well, work
measuring	9	69	1.64	absence, bit, dark, end, first, information, measured, measuring, metric, point, risk, scale, set, shading, someone, stage, standard, start, step, test, utility, value, years
change	6	116	1.63	action, add, address, align, assist, back, better, bring, change, clarification, clean, clear, colour, colouring, construct, development, draw, end, even, fall, figure, fit, focus, following, green, illustrate, improve, improvement, introduction, investment, issue, level, make, mark, mitigation, organization, part, point, process, produce, provide, recommend, recover, represent, right, scale, section, secure, set, stage, start, step, sub, take, test, thing, think, validate, work
work	4	87	1.43	action, analysis, answer, apply, assist, bring, colour, complex, detection, inquiry, issue, make, makes, manage, model, part, place, project, read, reference, represent, research, risk, set, solve, take, tell, treatment, understand, use, utility, work
someone	7	61	1.39	analyst, better, broad, consultant, draw, engineer, expert, figure, great, green, image, issue, major, manager, mark, member, model, modern, name, practitioner, professional, reader, regular, researcher, senior, someone, tell, type, user, warren, wise
good	4	61	1.25	artefact, better, change, consideration, depends, estimation', expert, future, generic, good, great, respective, right, secure, security, solid, well
figure	6	66	1.17	add, assess, design, designed, digital, estimation', evaluate, expert, figure, idea, image, make, mark, model, name, one, place, process, reason, reckon, representation, set, shading, single, solve, standard, two

Figure 5.33: Generalisation of Top 10 Most Frequent Words (Level 5)

5.3.3 Text Search Result

After performing word frequency analysis, it is important to run "Text Search" queries in NVivo. This allows the researcher to discover all occurrences of a specific word, phrase, or concept in the text content of the expert feedback. NVivo supports this research by offering the following capabilities:

- Examining the usage, context, and significance of words, especially when specific expressions are predominantly used in a particular context.
- Automatically coding words or expressions.
- Searching for ideas and concepts that encompass similar words.

The results of text searches in NVivo are displayed in a tree structure, with branches representing the different contexts in which the word or phrase appears. Thus, the researcher can identify recurring themes or phrases that are associated with a specific word. This selection of words enables a deeper comprehension of the strengths of the proposed artefact and aids in discovering relevant that can be linked together, such as attributes of the artefact. These words include: “risk”, “risk identification”, “treatment”, “mitigation”, “monitoring”, “metric”, “improvement”, “strength”, and “good”. The words are reported with a commentary below.

The word “risk” appeared from the received feedback in a different context, including the framework phases, missing artefact components, and improvement as shown in Figure 5.34. More specifically, the word “risk identification” showed as an effective phase with data mapping as illustrated in Figure 5.35. It also requires further modifications to be aligned with the overall framework workflow.

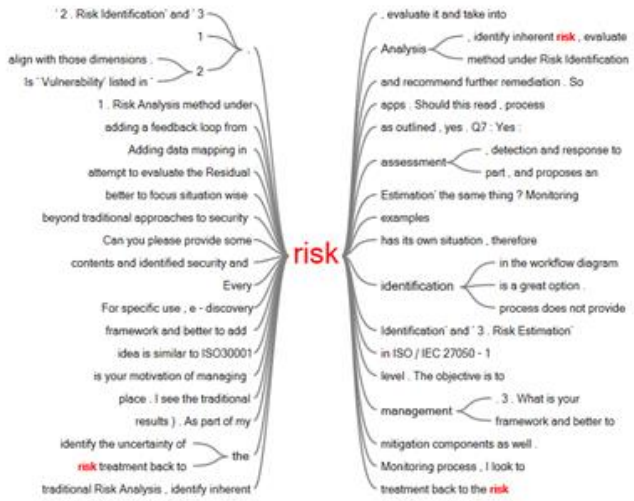


Figure 5.34: NVivo Text Search Criteria for "Risk"

Figure 5.35: NVivo Text Search Criteria for “Risk Identification”

Furthermore, both words “treatment” and “mitigation” appeared to be important aspects to consider when enhancing the proposed artefact as illustrated in Figure 5.36 and Figure 5.37. Similarly, Figure 5.38 and Figure 5.39 present two words “monitoring” and “metric” as missing components of the proposed artefact. This was demonstrated when searching for the word “improvement” as depicted in Figure 5.40.

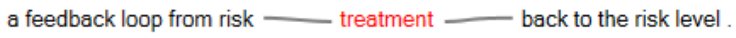


Figure 5.36: NVivo Text Search Criteria for “Treatment”

Figure 5.37: NVivo Text Search Criteria for “Mitigation”

Figure 5.38: NVivo Text Search Criteria for "Monitoring"

Figure 5.39: NVivo Text Search Criteria for "Metric"

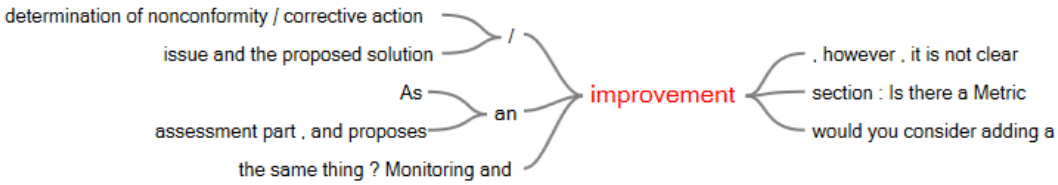


Figure 5.40: NVivo Text Search Criteria for "Improvement"

The last two words “strength” and “good” have been tested to confirm the suitability and effectiveness of the proposed artefact. Although the results presented in Figure 5.41 and Figure 5.42 do not show a tree with many branches (i.e., with linkable information), it is obvious from the previous analysis that the proposed artefact has the capabilities to be implementable in the eDiscovery environment.

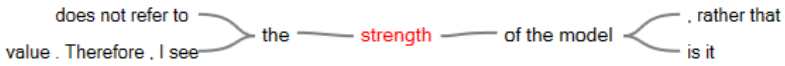


Figure 5.41: NVivo Text Search Criteria for "Strength"

Figure 5.42: NVivo Text Search Criteria for "Good"

From a different perspective, the NVivo tool helped the researcher to search for expressions of sentiment in expert feedback. It is an auto-coding functionality that performs opinion mining (i.e., subjective feedback of an expert to the proposed artefact). NVivo has a pre-defined sentiment scoring method as shown in Figure 5.43. It is worth noting that words with a score that falls within the neutral range are not coded.

Figure 5.43: Sentiment Scoring in NVivo

In this research, a combination of searching for sentiment and manual fine-tuning has been applied to code the sentiment of feedback as outlined in Table 5.5.

Table 5.5: Experts' Feedback and Sentiment Scoring

Very Positive (++)	*"I reckon it's solid" (Expert 1).* *"Therefore, I see the strength of the model is it provides a single point of reference, as a way into what are otherwise dense textual standards" (Expert 8).* *"It looks beyond traditional approaches to security risk assessment, detection, and response to manage a wider set of risks (Expert 10).*
Moderately Positive (+)	*"Every risk has its own situation, therefore it better to focus situation wise risk management framework and better to add risk mitigation components as well" (Expert 3).* *"The step looks logical" (Expert 4).*

	"All major components are listed. It is seamlessly linked to relevant security standards" (Expert 6). *"I see the traditional Risk Analysis, identify inherent risk, evaluate it, and take into consideration the existing controls, relevant incident, stakeholders' input, etc. Then, attempt to evaluate the Residual risk and recommend further remediation" (Expert 7).* *"I really like the model. From what I see, regardless of the standard being implemented e.g., NIST, ISO, or even in SOC2 type attestations, it can bring structure to the process stages" (Expert 8).* *"Adding data mapping in risk identification is a great option" (Expert 9).*
Moderately Negative (-)	*"As an improvement would you consider adding a feedback loop from risk treatment back to the risk level" (Expert 1).* *"As part of my Risk Monitoring process, I look to the objectives to set out what is to be monitored, how it is then measured, who does it, when and how that is sourced and evidenced" (Expert 2).* *"Every risk has its own situation; therefore, it is better to focus on situation wise risk management framework and better to add risk mitigation components as well" (Expert 3).* *"Risk identification process does not provide details about process of evaluating, measuring, and mitigating the many risks" (Expert 5).* *"I see the traditional Risk Analysis, identify inherent risk, evaluate it, and take into consideration the existing controls, relevant incident, stakeholders' input, etc. Then, attempt to evaluate the Residual risk and recommend further remediation" (Expert 7).* *"It attempts to address an issue, as I understood, to identify the uncertainty of the risk assessment part, and proposes an improvement, however, it is not clear at all how this will take place" (Expert 7).* *"I would suggest lighter shading, as when printed the dark green colouring of the model makes the inbox legends difficult to read" (Expert 8).*
Negative (- -)	*"Lack of clear definition of the issue the proposed framework attempts to solve" (Expert 7).*

It was reported that positive and negative sentences have the same code. For example, the quote from Expert 7: *"I see the traditional Risk Analysis, identify inherent risk, evaluate it, and take into consideration the existing controls, relevant incident, stakeholders' input, etc. Then, attempt to evaluate the Residual risk and recommend further remediation"* fall under both **Moderately Positive** and **Moderately Negative** score.

5.3.4 Suggested Changes

Based on the feedback received from the selected experts, some modifications will be made to improve the quality of the proposed Artefact 2. All recommended adjustments and amendments raised by the experts have been incorporated into the proposed Artefact 3. An iteration process has been identified to ensure that the recommended changes applied to the new version of the proposed Artefact 3 are linked with the previous version 2.

Table 5.6 provides a list of suggested changes that will be applied to the proposed Artefact 2. This list will be further elaborated in Section 5.4. It is important to note that the last three suggestions (Ch#11, Ch#12 & Ch#13) will not be applied as they are out of scope and will be part of a future improvement plan (as discussed in Section 7.4).

Table 5.6: Suggested Changes and Their References

Change#	Suggested Change	Reference(s)
Ch#01	Add a new activity to identify the Stakeholders before engaging them in the Asset identification activity.	Expert 2 provided this comment in a graphical presentation (see Figure 5.8).
Ch#02	Add the word 'Identification' next to the 'Vulnerability' component in the Risk Identification phase.	Expert 2: "Is 'Vulnerability' listed in '2.Risk Identification and '3. Risk Estimation' the same thing?"
Ch#03	Add the word 'Probability' next to the 'Vulnerability' component in the Risk Estimation phase.	Expert 2: "Is 'Vulnerability' listed in '2.Risk Identification and '3. Risk Estimation' the same thing?"
Ch#04	Add a feedback loop from the Risk Treatment phase back to the Risk Level component.	Expert 1: "As an improvement would you consider adding a feedback loop from risk treatment back to the risk level. The objective is to re-assess the level after being treated." (see Figure 5.5).
Ch#05	Add a 'Mertic Determination' component to the Monitoring & Improvement phase.	Expert 2: "Is there a Metric Determination?". Expert 2: "As part of my Risk Monitoring process, I look to the objectives to set out what is to be monitored, how it is then measured, who does it, when and how that is sourced and evidenced."

Change#	Suggested Change	Reference(s)
Ch#06	Add a 'Measure' component to the Monitoring & Improvement phase.	Expert 2: "As part of my Risk Monitoring process, I look to the objectives to set out what is to be monitored, how it is then measured, who does it, when and how that is sourced and evidenced."
Ch#07	Map the proposed framework phases with the ISO/IEC 27050 seven process phases (identification, preservation, collection, processing, review, analysis, and production).	Expert 5: "The framework dimensions must be comprehensively around identified, protect, detect, respond, and recover". Expert 8: "What would assist usability is perhaps if there was an alignment with the labels across both diagrams including the 1 through 5 process steps. Perhaps providing a lighter colour coding per step that ties back to Figure 1 would assist".
Ch#08	Revisit the risk management principles to ensure they are aligned with the ISO/IEC 27050 standard.	Expert 4: "2. The framework idea is similar to ISO31000 Risk Management. 3. What is your motivation for managing Risk in ISO/IEC 27050-1?".
Ch#09	Change the arrow on the left side of the 'Risk Analysis Method' component to an 'out' rather than 'in'.	Expert 2 provided this comment in a graphical presentation (see Figure 5.8). Expert 9: "Risk Analysis method under Risk Identification in the workflow diagram does not lead to a next step and the method is not identified".
Ch#10	Make arrowheads coming out and coming in both 'Threat Capability' and 'Control Strength'.	Expert 2 provided this comment in a graphical presentation (see Figure 5.8).
Ch#11	Identify a list of metrics aligned with the risk management objectives.	Expert 2: "As part of my Risk Monitoring process, I look to the objectives to set out what is to be monitored, how it is then measured, who does it, when and how that is sourced and evidenced."
Ch#12	Add a 'Method Selection' component to the Monitoring and Improvement phase.	Expert 2: "Perhaps a 'Method Selection' leading to here (which ideally would be designed to produce comparable and reproducible results)".
Ch#13	Add an 'Internal Audit' component to the Monitoring and Improvement phase.	Expert 2: "Mainly, there are regular internal audits, providing a determination of nonconformity / corrective action/improvement".

5.4 ARTEFACT 2 EVALUATION

After completing the expert evaluation analysis, the researcher has iterated back to the proposed Artefact 2 to make the required adjustments and improvements. Therefore, below is a list of improvements proposed to Artefact 2 based on the suggested changes described in Section 5.3.4 to design Artefact 3:

- Adding new components to the security risk management framework, including a 'Stakeholder Definition' component in the Context Establishment phase and 'Metric' and 'Measure' components in the Monitoring and Improvement phase.
- Adding the term 'Engagement' next to the 'Stakeholder' component in the Risk Identification phase, 'Identification' next to the 'Vulnerability' component in the Risk Identification phase, and 'Probability' next to the 'Vulnerability' component in the Risk Estimation phase.
- Adding a feedback loop from the 'Risk Acceptance Options' in the Risk Evaluation and Treatment phase back to the 'Risk Level' component in the Risk Estimation phase.
- Fixing the arrows and arrowheads in multiple locations, including the 'Risk Analysis Method' component in the Risk Identification phase, the 'Threat Capability' and 'Control Strengh' components in the Risk Estimation phase.
- Creating a mapping between the eDiscovery process phases and the proposed security risk management process phases.
- Aligning the risk management principles with the ISO/IEC 27050 standard.
- Adjusting all Artefact 3 relevant diagrams as required, including security risk management principles, framework style, process, and ArchiMate 3.1 metamodel.

5.5 IMPROVED FRAMEWORK AND ARTEFACT 3

An iteration process has been identified to ensure that the proposed improvements outlined in Sections 5.3.4 and 5.4 are applied to the new version of the proposed artefact, and are linked with the previous version of Artefact 2.

The feedback obtained from the experts' evaluation is utilised to enhance the proposed framework and create Artefact 3 as illustrated in Figure 5.44. The red lines and boxes represent the modified arrows, amended words, and new components introduced in the proposed framework that contributed to the overall improvement.

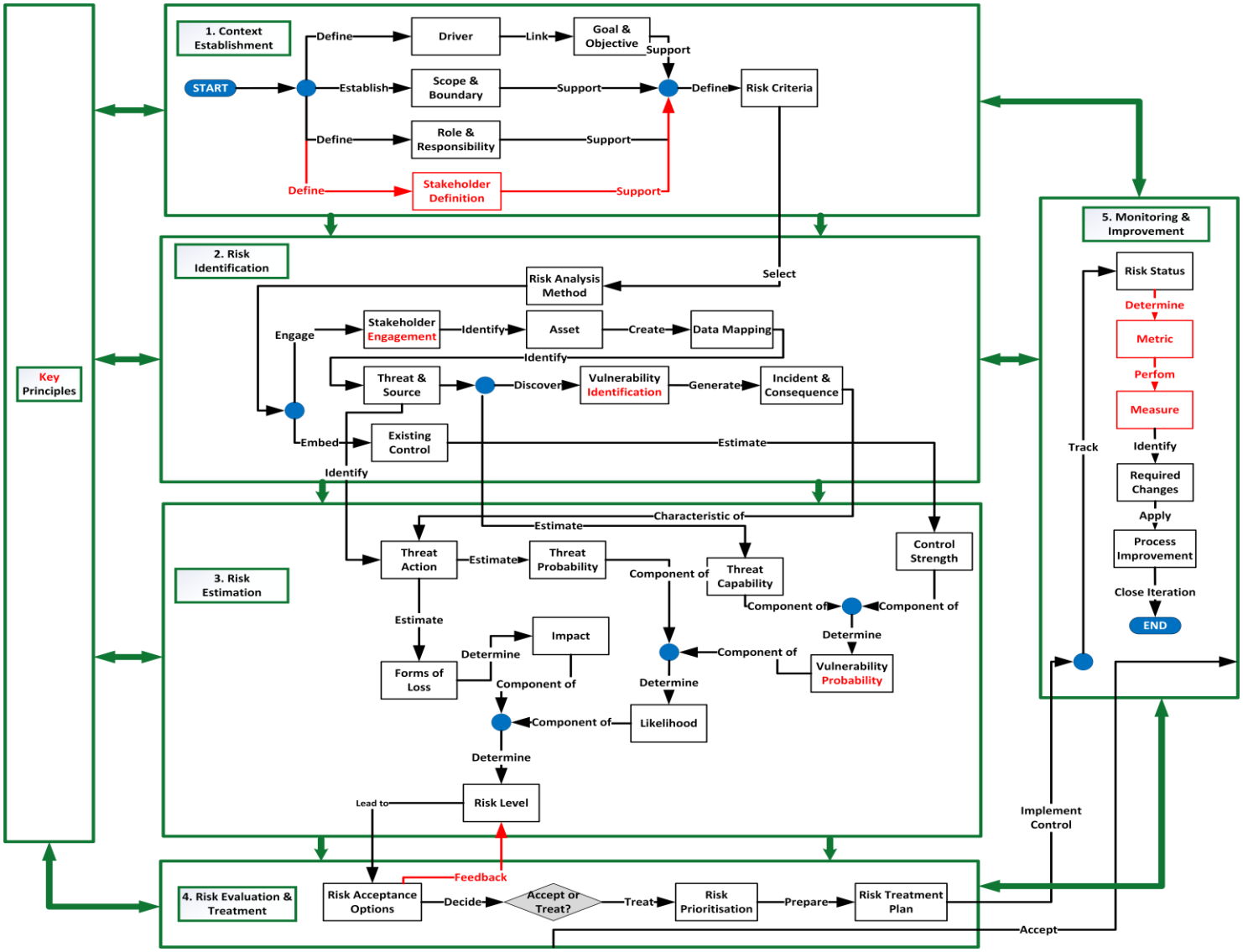


Figure 5.44: Improved Security Risk Management Framework (Artefact 3)

The following subsection provides more details about the major differences between Design 2 and Design 3 in terms of changes and adjustments made to improve the proposed security risk management framework.

5.5.1 Artefact 2 and Artefact 3

Figure 5.44 presents the Artefact 3 workflow (with several phases and their relevant components) after applying the required modification to Artefact 2.

Defining the 'Stakeholders' and then engaging them are important activities of the framework process. Artefact 2 considers only the engagement activity and misses the definition activity. This was a gap in terms of the process workflow. To close this gap as part of a process improvement (Artefact 3), the researcher applied two changes:

- Added a new activity called 'Stakeholder Definition' to identify the 'Stakeholder' after defining the 'Role & Responsibility' in the Context Establishment phase
- Added the term 'Engagement' after the term 'Stakeholder' to give more clarity about the expected activity and to ensure the security analysts define the 'Stakeholder' before engaging them in the Asset identification activity.

In Artefact 2, the 'Vulnerability' activity appeared in two phases: Risk Identification and Risk Estimation. This confuses the reader and does not provide any clear distinction between the two activities. To close this gap, the researcher made small changes to Artefact 2 by adding the term 'Identification' in the first activity and the term 'Probability' in the second activity. The key differentiation between the two activities is that Vulnerability Identification involves various categories such as organisation, processes and procedures, management routines, personnel, physical environment, information system configuration, hardware, software, or communications equipment, while the Vulnerability Probability refers to the likelihood that a threat event will result in a loss event.

In Artefact 2, there was a missing linkage between the Risk Estimation phase and Risk Evaluation & Treatment phase. To resolve this issue, the researcher added a feedback loop from the 'Risk Acceptance Options' activity back to the 'Risk Level' component. This is to ensure that the risk level will be re-assessed after being treated.

The Monitoring and Improvement phase represents a crucial part of the security risk management framework. Metrics play a vital role in the security risk management

framework, enabling organisations to quantify, direct, control, and improve the overall security maturity level. Artefact 2 does not address the security metrics. To overcome this gap, the researcher added two activities: determining 'Metric' and performing 'Measure' to provide appropriate information relating to decisions concerning security risks. Adding the activities above improved Artefact 2. However, Artefact 3 does not intend to provide guidelines in defining the appropriate metrics/measurement methods or assisting organisations in evaluating the effectiveness of security controls. This is out of the scope of the proposed security risk management framework.

The Artefact 2 does not show how the proposed security risk management framework is mapped to the ISO/IEC 27050 seven process phases (i.e., identification, preservation, collection, processing, review, analysis, and production). Section 5.5.2 discusses how the mapping is captured as part of the Artefact 3 structure. The changes were made to the Artefact 2, and the researcher revisited the defined risk management principles to ensure they are aligned with the ISO/IEC 27050 seven process phases. Artefact 3 has nine improved principles with a newly added principle (i.e., ten principles in total). This adjustment is explained in Section 5.5.3.

From an improvement perspective and based on the expert feedback, in the Risk Identification phase, the arrow on the left side of the 'Risk Analysis Method' component was changed from an 'in' to an 'out'. Furthermore, in the Risk Estimation phase, arrowheads coming out and coming in are made in both 'Threat Capability' and 'Control Strength' activity.

To reflect the changes above, a set of adjustments made to Artefact 2 are as follows:

- An improved framework is discussed in Section 5.5.4.
- An improved security risk management process diagram after adding the new components and applying the required adjustments as described in Section 5.5.5.
- An improved ArchiMate 3.1 metamodel diagram as explained in Section 5.5.6.

5.5.2 Electronic Discovery Process and Artefact 3 Integration

The main objective of an integration process is to combine multiple things into one. Integration is the act of connecting various standardised processes into a unified process that shares common elements, intending to enhance the overall effectiveness of the process. Integration can be seen as a distinct process that demands additional effort, yet

it brings numerous benefits and a broad array of advantages, including a cohesive set of interconnected processes (Rebelo et al., 2016). In this research, the integration involves the interlink at each of the eDiscovery phases with all security risk management activities/components being undertaken.

5.5.2.1 Integration Approach

In the context of this research, the proposed security risk management is linked to the eDiscovery domain. This is achieved through a systematic approach as illustrated in Figure 5.45 and detailed below.

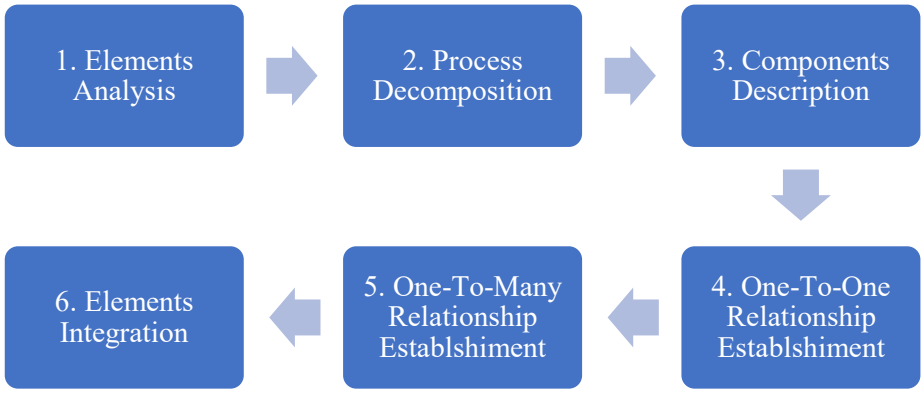


Figure 5.45: Integration Approach

- **Step 1 – Elements Analysis**: Understand and analyse the eDiscovery process elements, concepts, and their interrelationship from all ISO/IEC 27050 standard series.
- **Step 2 – Process Decomposition**: Decompose the ISO/IEC 27050 lifecycle into its components of each phase of the eDiscovery process based on the tasks associated with the appropriate eDiscovery process elements as explained in the Technical Readiness of ISO/IEC 27050 standard (Part 4). The technical readiness represents both requirements and guidance for proactive measures that enable an effective eDiscovery implementation as detailed in the Code of Practice of ISO/IEC 27050 standard (Part 3).
- **Step 3 – Components Description**: Describe in brief the identified components of the required tasks for each phase of the eDiscovery. This may include knowledge, skills, activities, and technologies.
- **Step 4 – One-To-One Relationship Establishment**: Create a one-to-one relationship in which each phase in the eDiscovery process is mapped to a list of components for each phase of the security risk management phase:

- To which is an eDiscovery phase mapped to single or multiple phases of the security risk management phases?
- If there is a mapping found, then what are the associated components of each security risk management phase that addresses the mapped eDiscovery phase?

These answers present the integration points between the current ISO/IEC 27050 standard and the proposed Artefact 3.

- **Step 5 – One-To-Many Relationship Establishment**: Create a one-to-many relationship between the eDiscovery components and applicable security risk management components. Which component in eDiscovery is associated with a component in a security risk management phase?
- **Step 6 – Elements Integration**: Integrate the new elements above into the security risk management building blocks:
  - What kind of alignment needs to be performed for each risk management principle?
  - What are the eDiscovery components that need to be interacted with to establish the foundations of the overall security risk management framework?
  - How the cross-activities will be integrated to establish, identify, estimate, and evaluate risk in the eDiscovery domain?

5.5.2.2 Security Risk Management and ISO/IEC 27050 Integrated Model

The eDiscovery process consists of seven main phases: identification, preservation, collection, processing, reviewing, analysis, and production. Aftering analysing the processes a set of components was identified for each phase as depicted in Figure 5.46. Furthermore, a high-level description of each component has been created and provided in Table 5.7. They were described based on the ISO/IEC 27050-4 standard and its associated standards: ISO/IEC 27050-1, ISO/IEC 27050-2, and ISO/IEC 27050-3 (refer to Section 2.5, Table B6.1 and Table B6.2 in Appendix B6).

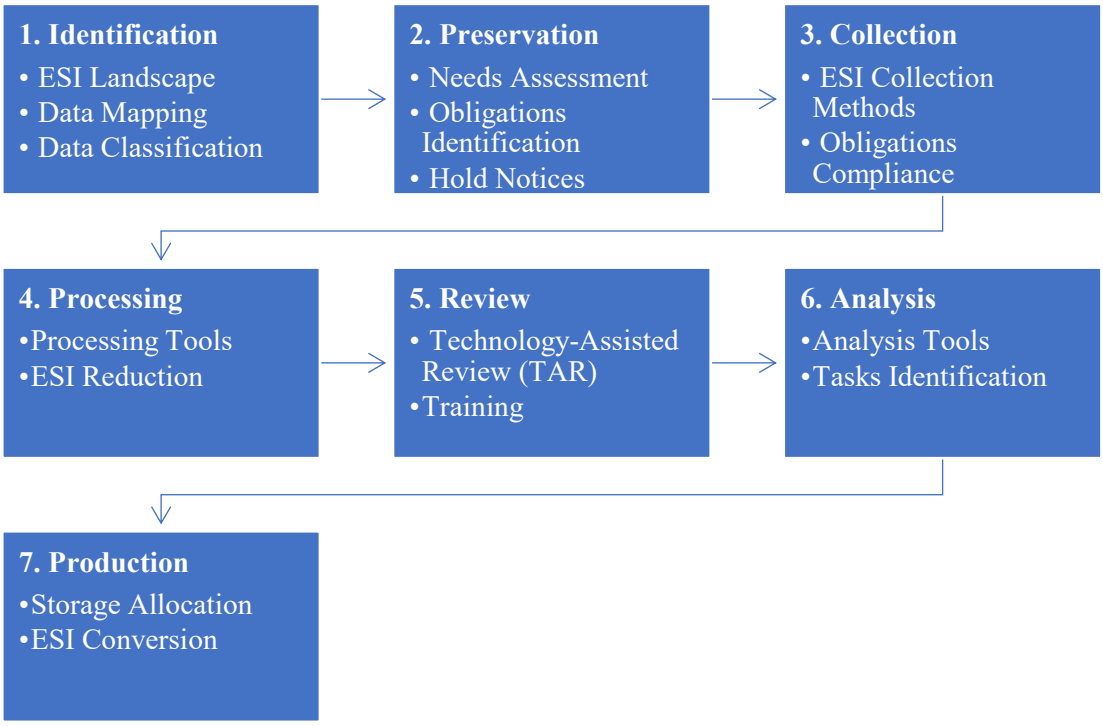


Figure 5.46: Electronic Discovery Process Phases with their Components

Table 5.8 presents the integration between the security risk management framework and the eDiscovery process. It shows a one-to-one relationship in which each phase in the eDiscovery process is mapped to a list of components for each phase of the security risk management phase. For example, the 'Asset' and 'Data Mapping' components in the Risk Identification phase (in a row) are mapped to the Identification phase (in a column).

Furthermore, other observations are reported in Table 5.8. It is noticed that there is a case in which mapping is not applicable because there is no relationship between the two processes. For instance, there is no mapping between the Risk Estimation phase (in a row) and the Identification phase (in a column). The reason is that Risk Estimation focuses on the risk analysis activities using the FAIR model. The Identification phase for ESI activities does not include any activity relevant to the risk calculation. The Risk Estimation phase was introduced to close the gap in the eDiscovery process.

Secondly, the Context Establishment phase (in a row) is mapped to all seven eDiscovery phases. It is either fully mapped as shown in the Identification and Analysis phase or partially mapped as shown in the Preservation, Collection, Processing, Review, and Production phase. Thirdly, there is a single component only applicable for mapping, 'Control Strength' in the Risk Estimation phase and 'Risk Treatment Plan' in the Risk Evaluation & Treatment phase. Fourthly, both 'Mertic' and 'Measure' components in the

Monitoring & Improvement phase are only mapped to the ‘Analysis’ phase. This is because the ‘Analysis’ is an activity that can be undertaken in support of any of the iterative phases in the eDiscovery process.

Table 5.9 provides a one-to-many relationship between the eDiscovery components and the corresponding security risk management components. For example, the ‘ESI Collection Methods’ is in two components of two different phases of the security risk management process: the ‘Scope & Boundary’ in the Context Establishment phase and ‘Existing Control’ in the Risk Identification phase.

Table 5.7: Electronic Discovery Process Phases and Components Description

Phase	Components	Description
1. Identification	ESI Landscape	Identify potential sources of relevant ESI, including business units, teams, ICT systems, and hardcopy.
	Data Mapping	Create a data map with a comprehensive and defensible inventory of an organisation's ICT systems that store ESI (e.g., locations, data sets).
	Data Classification	Classify ESI based on government standards, market sensitivity, internal governance, privilege, data protection, or any matter requiring discovery.
2. Preservation	Needs Assessment	Assess the needs for a continued preservation process about where the relevant ESI is stored and technical implications of collection, including scope, number of subjects affected, who is required to act, who can control ESI, and the period for preservation.
	Obligations Identification	Understand preservation triggers within relevant jurisdictions and apply security measures to ensure the integrity of relevant ESI.
	Hold Notices	Follow a legal hold process (i.e., identify, locate, and preserve hardcopy, and ESI) relevant to a particular matter to prevent the deletion, destruction, or modification of ESI and information by individuals.
3. Collection	ESI Collection Methods	Select tools and methods appropriate to ESI collection to maintain the integrity of the ESI metadata (i.e., the material can be used as evidence where required).
	Obligations Compliance	Comply with data protection, privacy, or security obligations to protect data when it is in transit (transferred) or at rest (stored).
4. Processing	Processing Tools	Use tools to retrieve the ESI from the collected sources (e.g., tapes and backups) to ingest the various formats (e.g., legacy mail formats, legacy files), and to convert the native ESI to a more usable form.
	ESI Reduction	Document the specific tools and techniques used for ESI reductions with appropriate processes that are repeatable and provide consistent results.
5. Review	Technology-Assisted Review (TAR)	Use a computerised system (as part of the Technology Assisted Review "TAR" process) to code a collection of ESI that harnesses human judgments to distinguish relevant from non-relevant ESI.
	Training	Ensure the seed set or initial training set is appropriate for the matter.
6. Analysis	Analysis Tools	Use tools (with content and visual analytic capabilities) during the initial analysis and identification of documents to be collected to track the types and locations of relevant ESI.
	Tasks Identification	Identify common tasks relevant to ESI analysis to determine relationships and patterns among the data, make predictions, present visualisations of the data, or create reports to exercise judgement regarding the data.
7. Production	Storage Allocation	Allocate sufficient storage space for ESI production such that the ESI data sets can be staged.
	ESI Conversion	Use tools that allow for the conversion of ESI from native format to near-image or image formats.

Table 5.8: Integration between Electronic Discovery Process Phase and Security Risk Management Phases

	Security Risk Management Phases				
eDiscovery Phases	**1. Context Establishment**	**2. Risk Identification**	**3. Risk Estimation**	**4. Risk Evaluation & Treatment**	**5. Monitoring & Improvement**
1. Identification	- Driver - Scope & Boundary - Role & Responsibility - Stakeholder Definition - Goal & Objective	- Asset - Data Mapping	N/A	N/A	N/A
2. Preservation	- Driver - Scope & Boundary - Role & Responsibility - Goal & Objective	- Existing Control - Asset - Data Mapping	- Control Strength	- Risk Treatment Plan	N/A
3. Collection	- Role & Responsibility - Goal & Objective	- Existing Control	- Control Strength	- Risk Treatment Plan	N/A
4. Processing	- Scope & Boundary - Role & Responsibility	N/A	N/A	N/A	N/A
5. Review	- Scope & Boundary - Role & Responsibility	N/A	N/A	N/A	N/A
6. Analysis	- Driver - Scope & Boundary - Role & Responsibility - Stakeholder Definition - Goal & Objective	- Existing Control - Asset - Data Mapping	- Control Strength	- Risk Treatment Plan	- Metric - Measure
7. Production	- Scope & Boundary	- Existing Control	- Control Strength	- Risk Treatment Plan	N/A

Table 5.9: One-to-Many Relationships between Electronic Discovery Components and Applicable Security Risk Management Components

ESI Phases		Security Risk Management Phases											
		1. Context Establishment					2. Risk Identification			3. Risk Estimation	4. Risk Evaluation & Treatment	5. Monitoring & Improvement	
Process	Components	Driver	Scope & Boundary	Role & Responsibility	Stakeholder Definition	Goal & Objective	Existing Control	Asset	Data Mapping	Control Strength	Risk Treatment Plan	Metric	Measure
1. Identification	ESI Landscape	☑	☑	☑	☑	☑							
	Data Mapping							☑	☑				
	Data Classification							☑	☑				
2. Preservation	Needs Assessment		☑	☑				☑	☑				
	Obligations Identification	☑				☑	☑				☑		
	Hold Notices			☑			☑			☑	☑		
3. Collection	ESI Collection Methods		☑				☑				☑		
	Obligations Compliance					☑	☑			☑	☑		
4. Processing	Processing Tools		☑										

ESI Phases		Security Risk Management Phases											
		1. Context Establishment					2. Risk Identification			3. Risk Estimation	4. Risk Evaluation & Treatment	5. Monitoring & Improvement	
Process	Components	Driver	Scope & Boundary	Role & Responsibility	Stakeholder Definition	Goal & Objective	Existing Control	Asset	Data Mapping	Control Strength	Risk Treatment Plan	Metric	Measure
	ESI Reduction		☑	☑									
5. Review	Technology-Assisted Review		☑	☑									
	Training		☑	☑									
6. Analysis	Analysis Tools	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	Tasks Identification		☑	☑				☑	☑		☑	☑	☑
7. Production	Storage Allocation		☑				☑				☑		
	ESI Conversion		☑				☑			☑	☑		

5.5.3 Improved Security Risk Management Principles

The Artefact 3 was improved based on ten overarching principles. Those principles were adopted and adapted based on general principles addressed in the ISO/IEC 31000 for risk management (refer to Section 3.5.2.1) and specific principles addressed in the ISO/IEC 30121 for digital forensic risk management (refer to Section 2.5). They are tailored to the processes of both eDiscovery and security risk management.

Table 5.10: Improved Security Risk Management Principles

No.	Principle	Description
1	Protection	Create and protect ESI organisation value.
2	Integration	Integrate and embed security risk activities with all eDiscovery process phases.
3	Systematic	Build a structured, comprehensive, and systematic method of security risk management for all eDiscovery process phases.
4	Alignment	Customise a security risk management framework and its components according to organisation objectives (e.g., external, and internal needs) and alignment with the eDiscovery process phases.
5	Responsibility	Involve related stakeholders as early as possible to understand and accept their responsibilities in respect of both eDiscovery process activities and security risk management processes.
6	Capability	Ensure the risk management can be dynamic, iterative, and responsive to change.
7	Quantitative	Consider all historical and current information and future expectations per the FAIR model.
8	Human Behaviour	Consider human and cultural factors, including the current and evolving needs of all the people in the security risk management processes.
9	Conformance	Comply with all compliance obligations, legal requirements, and other requirements per the organisation's risk criteria.
10	Continual Improvement	Facilitate continual improvement of security risk management.

Figure 5.47 shows the high-level alignment between the key principles and eDiscovery and risk management processes whereas Table 5.11 presents the mapping and relationship between the principles and the five security risk management processes and seven eDiscovery processes.

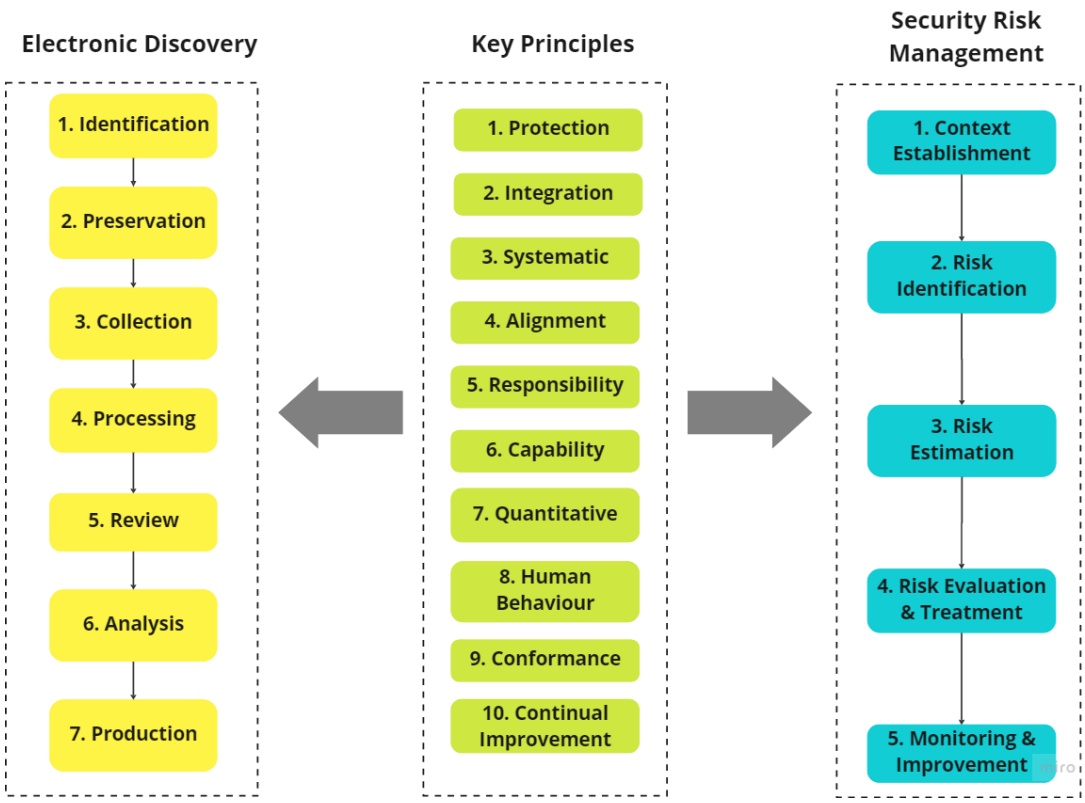


Figure 5.47: Principles Aligned with Electronic Discovery and Security Risk Management

Table 5.11: Principles and Processes of Security Risk Management and Electronic Discovery Relationship Mapping

	Security Risk Management					Electronic Discovery						
Principle	Context Establishment	Risk Identification	Risk Estimation	Risk Evalatuion & Tratement	Monitoring & Improvement	Identification	Preservation	Collection	Processing	Review	Analysis	Production
1. Protection	☑					☑	☑	☑	☑	☑	☑	☑
2. Integration	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
3. Systematic		☑	☑	☑		☑	☑	☑			☑	☑
4. Alignment	☑					☑	☑	☑	☑	☑	☑	☑
5. Responsibility	☑	☑				☑	☑	☑	☑	☑	☑	☑
6. Capability					☑						☑	☑
7. Quantitative	☑					☑	☑	☑	☑	☑	☑	☑
8. Human Behaviour	☑	☑				☑	☑	☑	☑	☑	☑	☑
9. Conformance	☑	☑	☑	☑			☑	☑				
10. Continual Improvement					☑						☑	

5.5.4 Improved Security Risk Management Framework

The security risk management framework has been improved with a set of newly added components to the Artefact 2: 'Stakeholder Definition', 'Metric', and 'Measure' that interact to produce the foundations of the overall framework as presented in Figure 5.48.

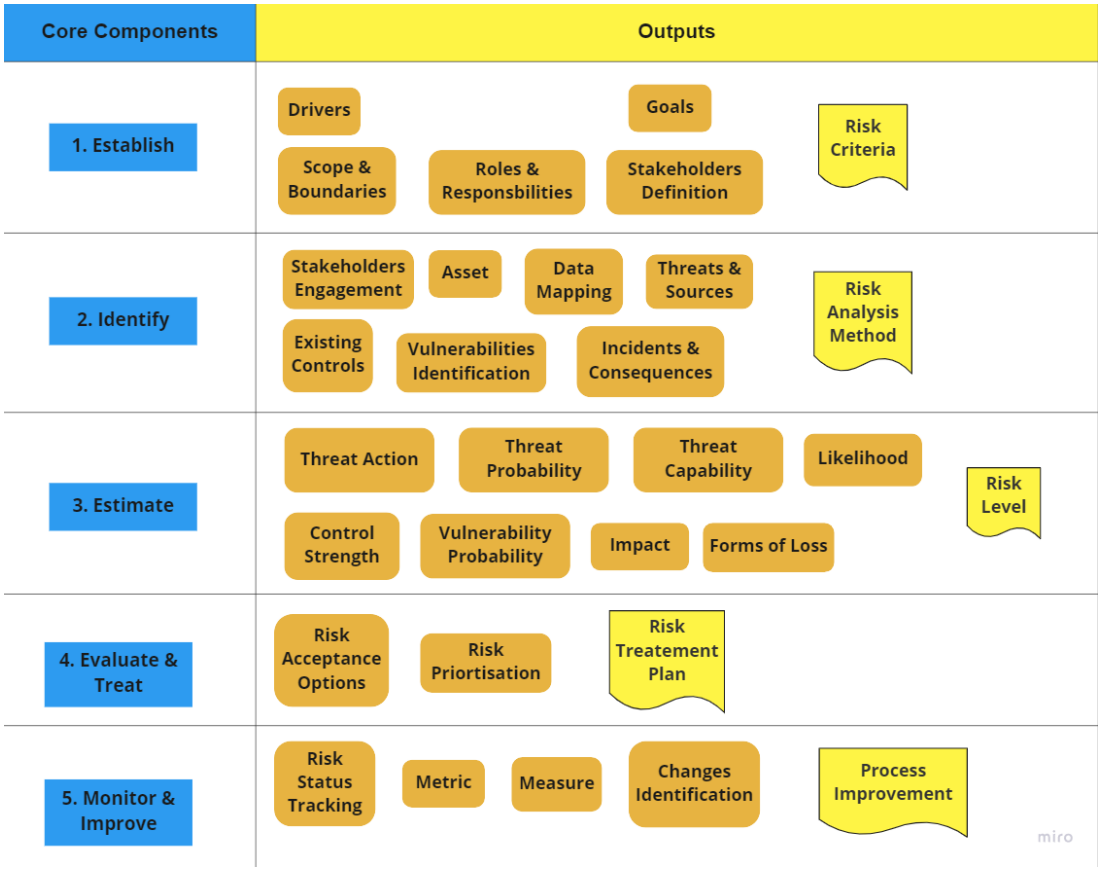


Figure 5.48: Improved Structural Core Components and Relevant Deliverables

5.5.5 Improved Security Risk Management Process

After adding the new components and applying the required adjustments, the security risk management process has been improved as illustrated in Figure 5.49.

A new activity (A1.5) has been added to the Context Establishment phase while two new activities (A5.2 & A5.3) have been added to the Monitoring and Improvement phase. Furthermore, the activity numbering and sequencing have been updated based on Artefact 3.

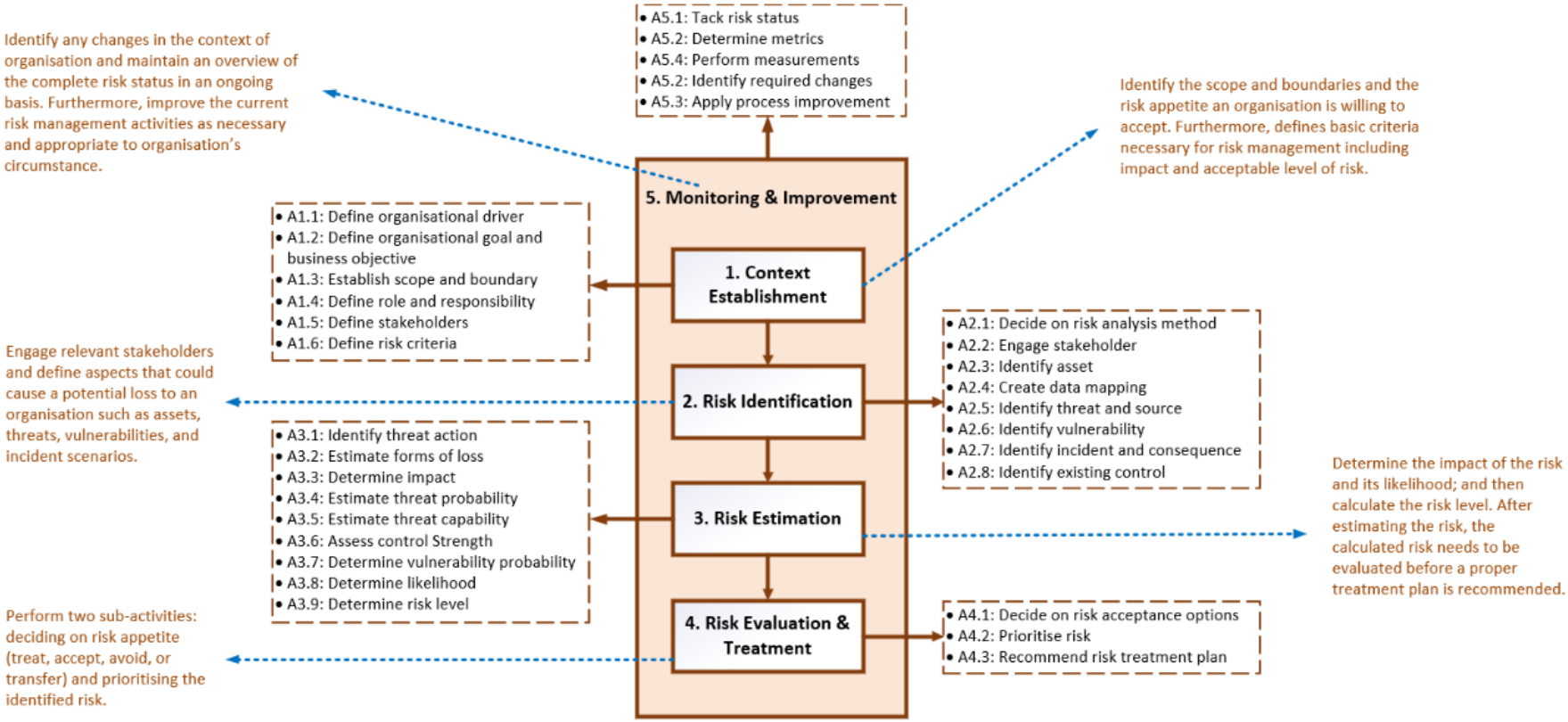


Figure 5.49: Improved Security Risk Management Process

Figure 5.50 presents the relationship between the security risk management conceptual model components: principles, framework, and process based on Artefact 3.

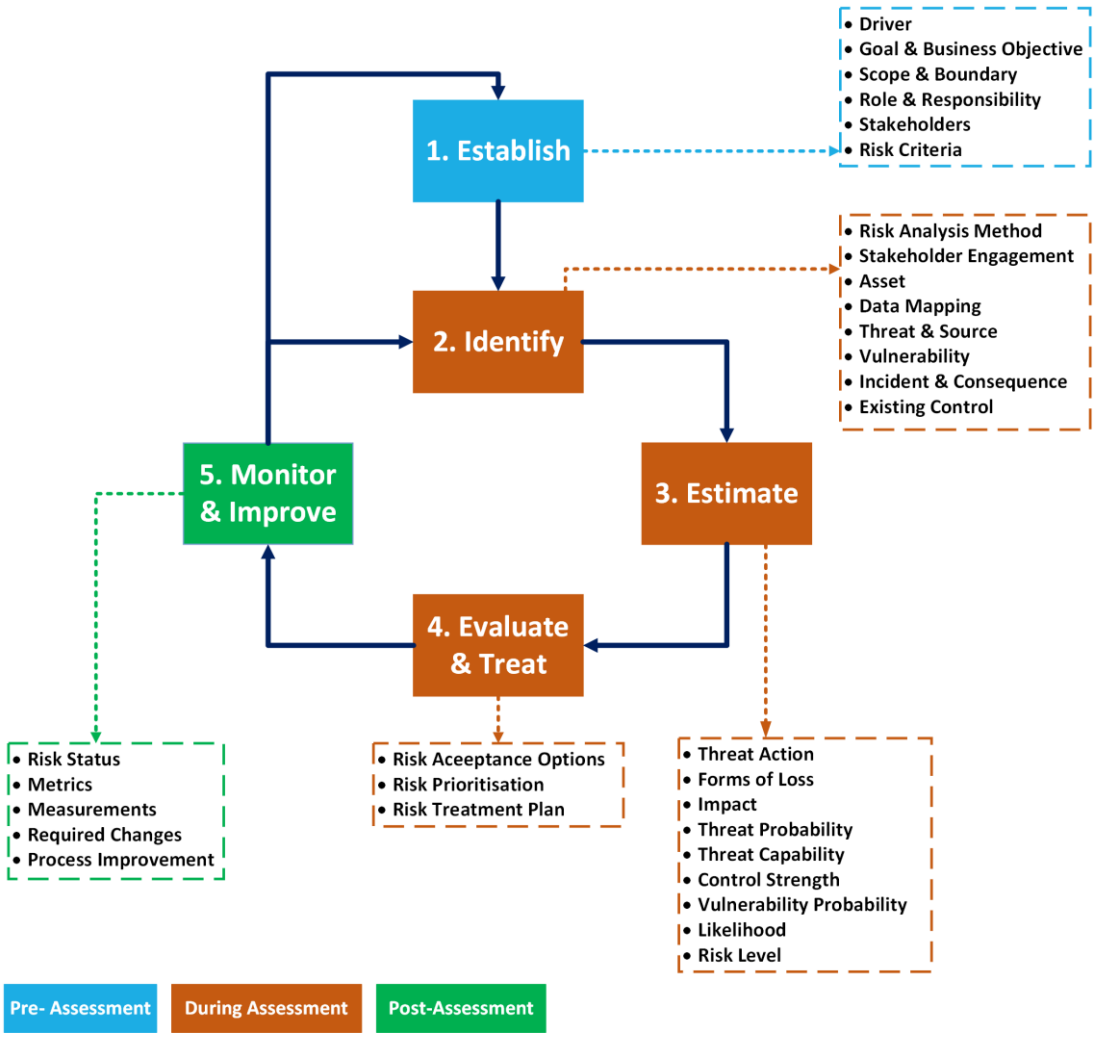


Figure 5.50: Improved Security Risk Management Principles, Framework and Process and their Relationship

Using the FAIR model as a computational engine in the Risk Estimation phase provides more benefits to organizations when measuring their risk. The FAIR model helps organisations make well-informed decisions through the following requirements (Jones, 2019):

- Establishing and evaluating assumptions.
- Ensuring consistent measurements when multiple risk analysts assess the same risk.
- Minimising personal bias and enhancing objectivity in measurements.
- Expressing risk calculations in a langue that is easily understood by organisational executives.

- Facilitating effective communication of the rationale behind risk estimations.
- Evaluating the cost-benefit proposition of risk management improvements.
- Efficiently utilise risk-related data.

5.5.6 Improved Security Risk Management Framework with ArchiMate 3.1 Metamodel

After adding the new components and applying the required adjustments, the security risk management framework ArchiMate 3.1 metamodel has been improved as illustrated in Figure 5.51.

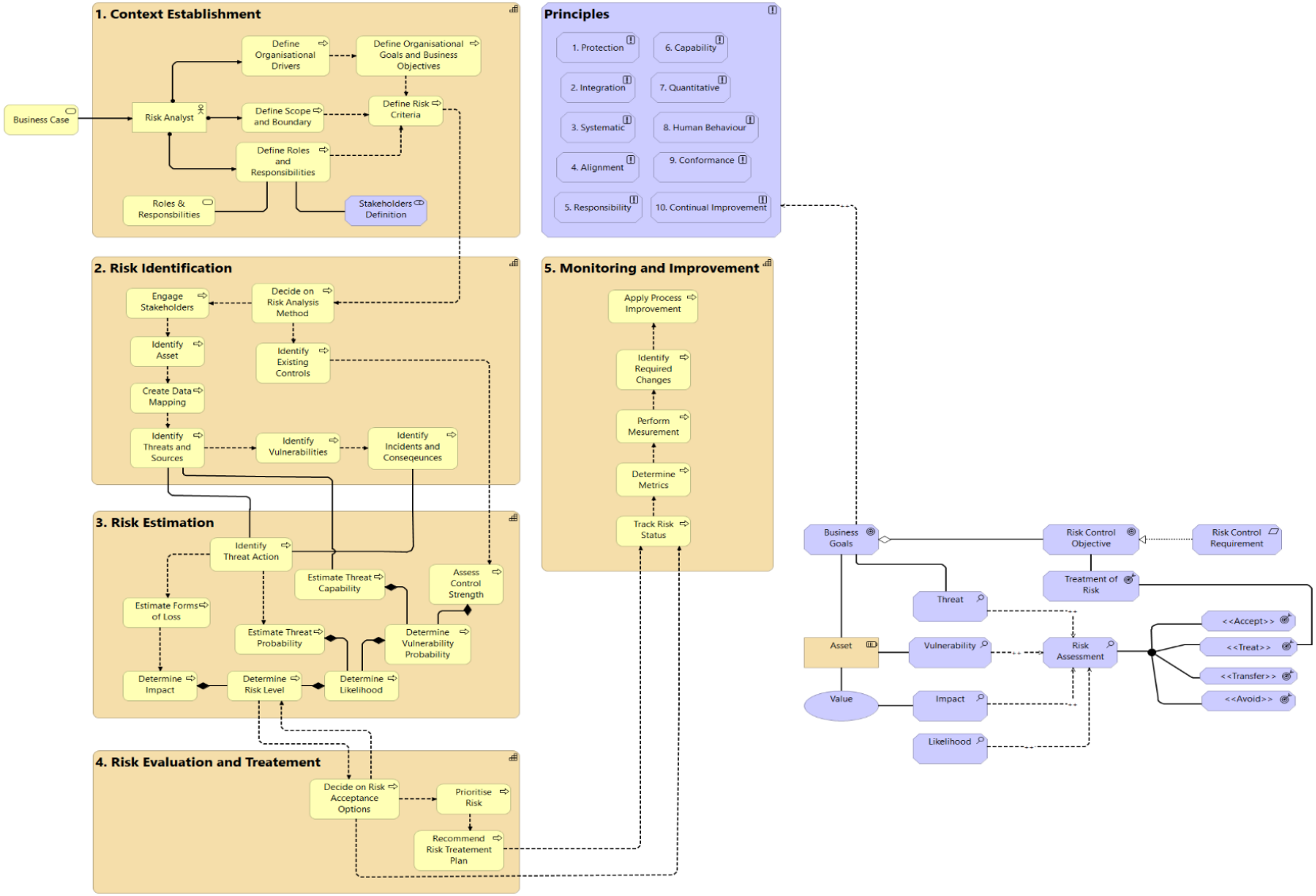


Figure 5.51: Improved Security Risk Management Framework ArchiMate 3.1 Metamodel

5.6 CONCLUSION

Evaluating artefacts aims to assess the extent to which they fulfil the requirements and address the identified problem that served as the motivation for the research.

Two types of evaluation were conducted: naturalistic and thematic evaluation. In naturalistic expert evaluation, a real test was conducted for the proposed artefact to evaluate its characteristics. Ten selected experts have been contacted to participate in evaluating the proposed artefact. A set of activities were carried out including creating an introduction letter, distributing a copy of the proposed security risk management framework diagram, and communicating a list of both open and closed starters to collect expert feedback. The expert feedback was collected; then assessed and analysed against eight criteria of the proposed artefact: efficacy, clarity, usefulness, alignment, usability, robustness, improvability, and completeness. Taking into account the feedback provided by the chosen experts, adjustments were made to enhance the quality of the proposed Artefact 2.

During the thematic evaluation, a qualitative research analysis was conducted using the NVivo tool. This included preparing a dataset, running word frequency queries "text search", and discovering all occurrences. After conducting the expert evaluation, the researcher has iterated back to the proposed Artefact 2 to make the required adjustments and improvements. A roadmap was proposed to improve Artefact 2 based on expert feedback. The researcher highlights the major differences between Artefact 2 and Artefact 3 in terms of changes and adjustments made to improve the proposed security risk management framework. More specifically, the improvements captured the various framework dimensions, including integration between the eDiscovery process and the proposed framework as well as framework principles, style, process, and the architecture model.

Finally, this chapter presents the third version of the proposed framework (Artefact 3) which is further discussed in Chapter 6. Therefore, Chapter 6 discusses the rationale between the primary research question, sub-questions, hypotheses, and findings.

Chapter 6: Discussion

6.0 INTRODUCTION

Figure 6.1 shows the summary of the thesis structure based on the proposed research methodology. The dashed lines show the roadmap for Chapter 6 and Chapter 7 which is Phase 6 (Artefact Results Demonstration).

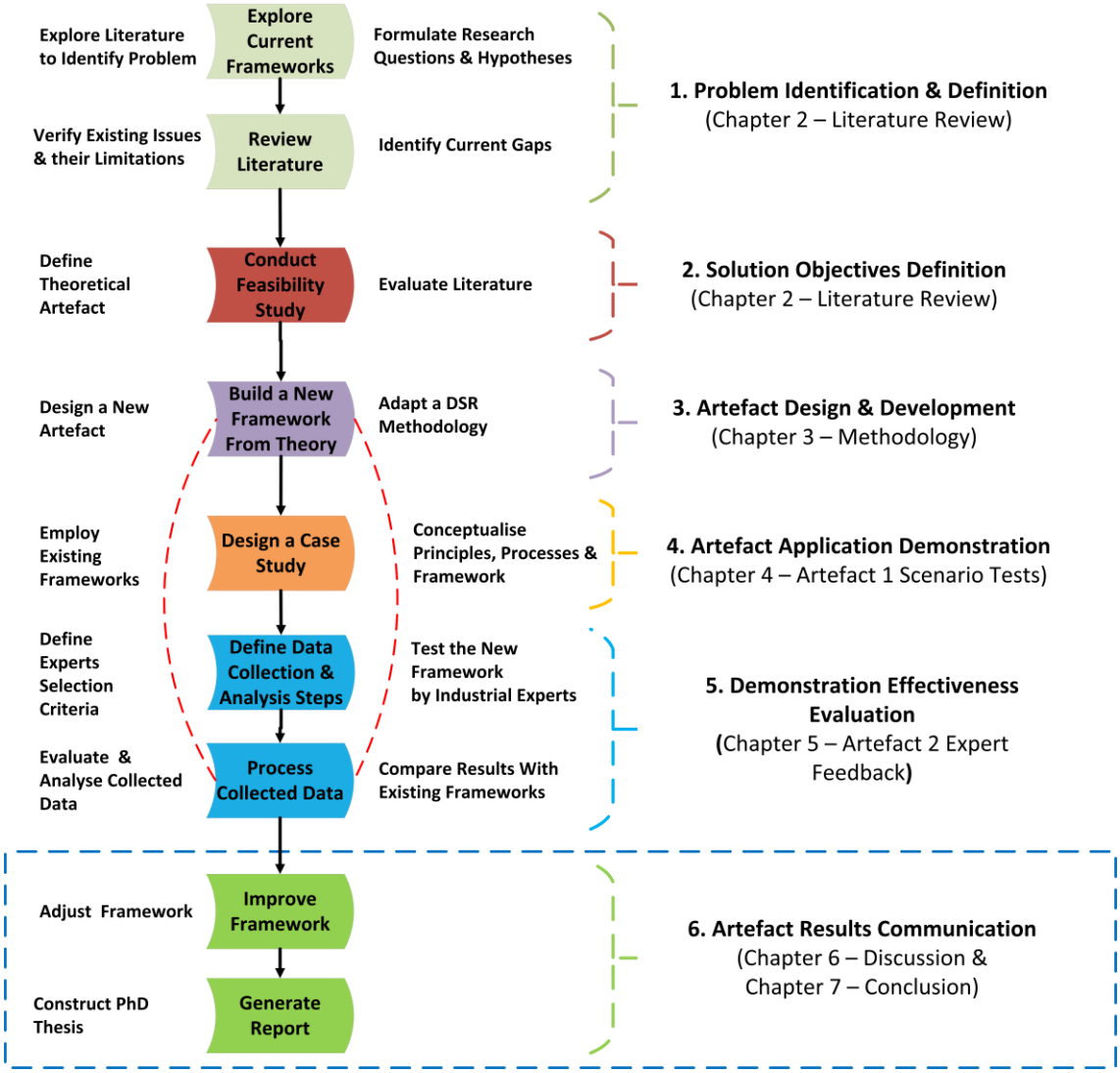


Figure 6.1: Chapter 6 Roadmap

To successfully conclude the research journey, it is important to establish the logical connections between the findings, research questions, and hypotheses, employing a Quasi-Judicial scholarly method. Chapter 6 focuses on evaluating the rationale that links the primary research question, sub-questions, hypotheses, and findings, spanning from Chapter 2 to Chapter 5.

This chapter is structured as follows. In Section 6.1, a rational argument is applied to prove or refute the defined hypothesis and answer the research sub-questions while Section 6.2 provides relevant evidence for each research hypothesis. Section 6.3 consolidates the answers gathered for each research sub-questions and hypothesis in Section 6.1 and Section 6.2. Furthermore, a graphical presentation is depicted at the end of Section 6.3. It demonstrates the relationship between the primary research question, sub-questions, and hypotheses and their associated answers. Section 6.4 connects the research findings and results with the literature that has been presented in the literature review in Chapter 2. Section 6.5 presents the research contribution to the body of knowledge for two main aspects: theory and eDiscovery practice. This chapter ends with the main conclusion and connection to Chapter 7 in Section 6.6.

6.1 ANSWERS TO RESEARCH SUB-QUESTIONS

The subsections below provide answers to the three research sub-questions based on the literature review, artefact development, testing, and evaluation. Moreover, those answers provide evidence to test the formulated hypotheses.

6.1.1 Sub-Question 1

In Chapter 3, Section 3.2.1, Sub-Question 1 was stated as follows: "*What are the main limitations and weaknesses of the current ISO/IEC 27050 standard in the context of risk management processes?*"

Based on the literature review in Chapter 2, Section 2.7.2, it has been found that the current ISO/IEC 2750 does not provide a detailed description of how to perform risk analysis and manage the identified security risks. Instead, it only provides high-level requirements for the whole ESI investigation process. While the ISO/IEC 27050 standard applies to both technical and non-technical tasks, its primary focus lies in addressing the requirements for regulatory and industry standards. This standard provides recommendations on effectively managing the ownership of risks associated with ESI, such as establishing and implementing the necessary policies to ensure compliance adherence. Although the ISO/IEC 27050 standard helps in identifying the risks associated with eDiscovery and then providing a basic mitigation plan, it does not provide a detailed description of how to perform risk analysis and manage the identified risks. Instead, it provides high-level requirements for the whole ESI investigation process.

Secondly, a risk management reference model was developed based on the three key analysis activities described in Chapter 2 as follows:

- Analysis of framework artefact of five frameworks and standards: ISO/IEC 31000, ISO/IEC 27005, NIST, ENISA, and The Risk IT (Section 2.4.7, Table 2.3, and Section 2.7.1).
- Analysis of the four ISO/IEC 27050 standard series: Overview and Concepts, Guidance for Governance and Management of Electronic Discovery, Code of Practice for Electronic Discovery, and Technical Readiness (Section 2.5 and Table B6.1 in Appendix B6).
- Analysis of risk management elements of three chosen frameworks: CURF, ISRA, and ISO/IEC 27005 (Section 2.7.2, Figure 2.10, and Table 2.5).

This reference model was used to perform a gap analysis through evaluation and assessment of the current state of the ISO/IEC 27050 standard in terms of the referenced risk management phases as outlined in Figure 2.10 and detailed in Table 2.5.

The assessment identifies the differences between the current state of the ISO/IEC 27050 standard and the risk management reference model. The outcome of the gap analysis indicated that 50% of the risk management reference model (11 activities) was not addressed within the ISO/IEC 27050 standard which represented a significant gap.

In conclusion, to answer Sub-Question 1, the current ISO/IEC 27050 standard does not have any sort of security risk management framework. At present, the eDiscovery guidelines ignore security risks and are populated by technical assistance for discovery. The use of these guidelines without a risk framework puts the users and the information at risk of disclosure and damage. Hence, the ISO/IEC 27050 standard has no security provisions for information protection.

6.1.2 Sub-Question 2

In Chapter 3, Section 3.2.1, Sub-Question 2 stated as follows: "*What design components improve the risk identification capabilities of the current ISO/IEC 27050 standard?*"

In Chapter 3, Section 3.5.2, the proposed framework aimed to close the gaps identified in Chapter 2 in the context of this research. It mainly addressed the missing tasks, activities, or processes within the evaluated risk management frameworks. On the other hand, in Chapter 3, the researcher has proposed a framework structure that is made of three main building blocks: principles, framework style, processes, and their relationship.

- Nine principles were proposed that provide guidance and a foundation for

enabling organisations to manage their risk (Section 3.5.2.1).

- A framework was built that has a set of components that interact to produce the foundations of the overall framework as presented in Figure 3.22. Five core components were introduced in which each component produces an output/deliverable that is used as an input for the next component (Section 3.5.2.2).
- A systematic process that is broken up into a series of actions or steps taken to establish, identify, estimate, evaluate, and treat risk (Section 3.5.2.3).

Secondly, in Chapter 3 and Chapter 4, a flexible and qualitative risk approach has been adopted and adapted (Section 3.4.4.3); and then integrated and embedded within the proposed security risk management framework (Section 4.4.1). New terminologies and processes were introduced to fit in the proposed security risk management framework ontology. The terminology and processes of the FAIR model new version have been reconciled to cater for the Risk Estimation process of the proposed security risk management framework in a consistent and repeatable manner as illustrated in Figure 3.21. Estimating risk using the FAIR model was performed through data/estimates at higher levels of abstraction within the model. The inherent flexibility of the FAIR model has enabled the risk analyst to choose a suitable level of analysis based on factors such as time, data availability, complexity, and significance of the scenario.

In Chapter 4, Section 4.4.2.2, the estimation of the risk level (ALE) involved deriving a series of functions that establish the relationships between variables (risk factors) and their respective sub-factors. These functions, whether static or probabilistic, represent the functional dependencies between each factor and its associated sub-factors. The factors and their corresponding functions were formulated and documented in Table D1.1 in Appendix D1. Generally, it has two key procedures: determining impact by aggregating Primary Loss and Secondary Loss and determining Likelihood by calculating Vulnerability and estimating Threat Probability. The ALE was calculated through the Monte Carlo simulator with simulated samples.

Thirdly, in Chapter 3, Section 4.4.2, ArchiMate 3.1 was used to provide a comprehensive architecture modelling language with graphical notation, relationships, and metamodel under three architecture layers: motivation, strategy, and business. A mapping between the proposed security risk management framework concepts and its

components with the ArchiMate 3.1 concepts has been modelled as exhibited in Figure 4.29.

In conclusion, to answer Sub-Question 2, the proposed security risk management framework has been constructed using the theoretical method explained in Section 3.5.2.4. This method started with building the intended framework from the literature analysis, developing three scenarios, testing the framework, and then getting the first feedback iteration completed. Based on the first feedback, the framework has been improved and then communicated to selected experts for their opinion. Next, the expert feedback has been further analysed through NVivo data analysis. Then, the final version of the framework has been improved based on the second feedback received from the experts.

6.1.3 Sub-Question 3

In Chapter 3, Section 3.2.1, Sub-Question 3 stated as follows: "*What steps are necessary to integrate the new artefact with the current ISO/IEC 27050 standard?*"

In Chapter 5, Section 5.5.2, an integration process was developed to integrate the proposed framework with the ISO/IEC 27050 standard. The integration involved the interlink at each of the eDiscovery phases with all security risk management activities/components. The proposed security risk management framework has been mapped to the eDiscovery domain.

The integration was performed through six steps as illustrated in Figure 5.45. The integration process started with understanding and analysing the eDiscovery process elements, concepts, and their interrelationship with all ISO/IEC 27050 standard series. The second step involved decomposing the ISO/IEC 27050 lifecycle into its components of each phase of the eDiscovery process based on the tasks associated with the appropriate Technical Readiness of eDiscovery process elements. A set of components has been identified for each phase of the eDiscovery process as depicted in Figure 5.46. The identified components have been briefly described in the third step which includes the required tasks for each phase of the eDiscovery process. This high-level description was presented in Table 5.7. The fourth step and fifth steps focused on building two key relationships. The first one was a one-to-one relationship in which each phase in the eDiscovery process has been mapped to a list of components for each phase of the security risk management as demonstrated in Table 5.8. The other one was a one-to-many relationship between the eDiscovery components and applicable security risk

management components as presented in Table 5.9. The integration process is completed by integrating the new elements into the security risk management building blocks: principles, framework style, and process.

Another dimension of integration was performed to embed and plugin the FAIR model into the Risk Estimation phase within the proposed security risk management framework as depicted in Figure 3.20. An adopted and adapted version of the FAIR model has been created to cater for the proposed risk management framework requirements as presented in Figure 3.21. This included two main aspects: focusing on the top-level and the middle-level of the standard FAIR model and introducing new terminologies to fit the proposed risk management framework ontology.

In conclusion, to answer Sub-Question 3, integrating the new Artefact 3 with the current ISO/IEC 27050 standard has been achieved through two integration dimensions: overall process dimension through the mapping between the eDiscovery components and the security risk management components; and risk estimation activities dimension using the new modified version of the FAIR model.

6.2 HYPOTHESIS TESTING

In Chapter 3, Section 3.2.2, a set of hypotheses were formulated to affirm the researcher's proposed artefact, which was developed based on the literature review in Chapter 2. This section examines the pertinent evidence found in the collected and analysed data from the expert feedback, along with the researcher's critical reflections on the expert feedback and the researcher's observations as presented in Chapter 5, Section 5.2.4. The relevant evidence is carefully referenced and examined to reach a verdict for the hypotheses, as demonstrated in Table 6.1, Table 6.2, and Table 6.3 respectively.

6.2.1 Hypothesis 1

Table 6.1 presents the evidence for and against Hypothesis 1 and the final verdict. Hypothesis 1 has a relationship with Sub-Question 1 and Sub-Question 2.

Table 6.1: Hypothesis 1 Testing

Hypothesis 1: *The proposed framework model adds value with a shift from the requirements approach to a referenced standards approach.*
Evidence For

In Chapter 2, Section 2.7.2, it was argued that the ultimate advantage of having a standardised risk management framework model is to have a common ground between different contexts in an eDiscovery domain. The analysis indicated that the current ISO/IEC 27050 standard does not provide a detailed description of how to perform risk analysis and manage the identified risks. To develop a fit-for-purpose framework, a research method process was executed using an ADSRM approach as explained in Chapter 3, Section 3.4.1.

The Artefact 1 testing scenarios were gathered in Chapter 4, Section 4.1, Section 4.2, and Section 4.3 respectively as well as the expert feedback and researcher's observations were obtained and articulated in Chapter 5, Section 5.2.3 and 5.2.4 respectively.

Table 5.2 contains a set of artefact evaluation criteria in Section 5.2.2.3 and their corresponding questions as follows:

- Usefulness to Workplace => Q3
- Usability and Implementation => Q5
- Robustness for Risk Management Improvement => Q6
- Advantages and Strengths => Q9

Most of the experts agree that the proposed security risk management framework has demonstrated a strong potential to be used in the eDiscovery domain. This framework can bring structure to the eDiscovery process phases (ESI lifecycle) by offering a single point of reference with a visual representation in contrast to other standards. The experts indicated that this is considered one of the strongest attributes of the proposed artefact. Furthermore, the framework looks beyond traditional approaches to security risk assessment, detection, and response, to manage a wider set of risks. This would help strategic cybersecurity leaders to demonstrate clear value in the organisation's cybersecurity investments.

In conclusion, the results obtained from the expert evaluation confirm that Artefact is a fit-for-purpose security risk management framework.

Evidence Against

Only Expert 7 indicated that the proposed artefact does not add value because it follows a traditional risk analysis process (refer to Section 5.2.4.3). However, Expert 7's opinion was not strongly against Hypothesis 1. No clear and direct statement contradicts the notion stipulated in Hypothesis 1 that shifting from a requirements approach to a referenced standards approach would add value.

Verdict => Accepted
A systematic literature method used in Chapter 2, an ADSRM approach applied in Chapter 3, scenarios tested in Chapter 4, and positive feedback received from the experts in Chapter 5 are strong evidence to support Hypothesis 1, leading to the conclusion that it is accepted (not rejected).

6.2.2 Hypothesis 2

Table 6.2 presents the evidence for and against Hypothesis 2 along with the final verdict. Hypothesis 2 has a relationship with Sub-Question 1.

Table 6.2: Hypothesis 2 Testing

Hypothesis 2: *The new artefact better identifies the risks associated with electronic discovery.*
Evidence For
The solution objectives of the proposal were listed in Chapter 2, Section 02.7.3, which includes the integration of the proposed framework model with the ISO/IEC 27050 standard. This model should be tailored to the eDiscovery process. It should also close the identified gaps in Chapter 2 by addressing the missing tasks, activities, or processes with the evaluated risk management frameworks. Chapter 3, Section 3.4.23.5.2 described the structure of the proposed model which consists of three building blocks: principles, framework style, and process and their relationship. The improved version of the proposed model was explained in Chapter 5, Section 5.5. Table 5.2 contains a set of artefact evaluation criteria in Section 5.2.2.3 and their corresponding questions as follows: • Efficacy for eDiscovery Risk Management => Q1 • Usability and Implementation => Q5 • Improvability of the Artefact => Q7 • Completeness and Modification => Q8 • Advantages and Strengths => Q9 Most of the experts acknowledged that the proposed security risk management framework could be useable in its current state. However, it has been observed that there was no clear one-to-one relationship between the eDiscovery process phases and the proposed artefact. This could be enhanced if there was an alignment with

the labels across both the proposed artefact diagram and the eDiscovery process diagram including the 1 through 5 process steps. To bridge this gap, the researcher has made a few adjustments to the proposed Artefact 2 by mapping between the security risk management framework and the eDiscovery process. A one-to-one relationship in which each phase in the eDiscovery process is mapped to a list of components for each phase of the security risk management phase. This mapping was presented in Table 5.8 and Table 5.9. In conclusion, the results obtained from the expert evaluation confirm that Artefact 2 with the new adjustment improves the risk identification process in the eDiscovery field.
Evidence Against
Only Expert 8 indicated that the proposed artefact does provide a clear alignment with the eDiscovery process (refer to Section 5.2.3.8 and Section 5.2.4.5). However, the identified gap was rectified and remediated in the improved Artefact 3. There is no reference or evidence found that refutes the stated Hypothesis 2.
Verdict => Accepted
Solution objectives described in Chapter 2, an ADSRM approach applied in Chapter 3, framework building blocks proposed in Chapter 3, noted positive feedback received from the experts in Chapter 5, and the improved Artefact 3 in Chapter 5 provide sufficient evidence that Hypothesis 2 cannot be rejected.

6.2.3 Hypothesis 3

Table 6.3 presents the evidence for and against Hypothesis 3 and the final verdict. Hypothesis 3 has a relationship with Sub-Question 1, Sub-Question 2, and Sub-Question 3.

Table 6.3: Hypothesis 3 Testing

Hypothesis 3: *The new artefact is a cost-effective risk identification method for organisations.*
Evidence For
The solution objectives of the proposal were listed in Chapter 2, Section 2.7.3, which includes the alignment with the international best practices. Alignment is one of the key principles of the proposed framework towards achieving the overall

organisation's objectives. Table 3.5 in Chapter 3 and Table 5.10 in Chapter 5 described the “alignment” as the proposed framework and its components should be customised according to organisation objectives (e.g., external, and internal needs) and aligned with the eDiscovery process phases.

Chapter 3, Section 3.4.4 provides an overview of the advantages of employing the FAIR model for risk estimation, specifically in terms of quantifying the financial implications associated with the assessed risks.

Table 5.2 contains a set of artefact evaluation criteria in Section 5.2.2.3 and their corresponding questions as follows:

- Alignment with International Security Risk Management Standards => Q4
- Robustness for Risk Management Improvement => Q6
- Advantages and Strengths => Q9

Most of the experts agree that the proposed artefact is aligned with numerous international standards including ISO/IEC 31000, ISO/IEC 27005, and NIST Risk Management Framework. It consists of all major components of a risk management framework. Moreover, it is seamlessly linked to relevant security standards, and it follows the PDCA model. It has been evident that the proposed Artefact 3 was customised and approached in a uniform way to achieve this alignment. This has provided a systemic and systematic understanding of the adopted and adapted standards and how the proposed Artefact 3 contributes to meeting the research goals including cost-effectiveness.

Introducing the FAIR model into the proposed Artefact 3 as a computational engine for assessing the probabilities and impacts of real risks improved the overall security risk management framework. This has shown that the proposed Artefact 3 has a well-structured framework to estimate and capture various costs and allocate them to risk scenarios. The integration enables organisations to effectively prioritise security risk, make informed trade-offs, calculate the ROI of security investments, and select cost-effective solutions to mitigate the identified risk. It has been evidence that the improved Artefact 3 helps organisations to:

- Identify the most critical security risks and quantify the potential exposure.
- Understand which investments in security risk management yield the highest value.
- Gain greater visibility into whether an organisation is allocating adequate or excessive resources to security risk management.

The series of functions and formulas used to calculate the overall risk has been developed and explained in Table D1.1 in Appendix D1. FAIR model is complementary to the proposed Artefact 3 that enables organisations to assess the significance and impact of identified and proposed improvements. It provides a framework to answer the question of "so what" by quantifying the potential consequences and implications of these factors. This integration allows organisations to gain a deeper understanding of the practical implications and make informed decisions based on the risk assessment provided by the FAIR model. In conclusion, the results obtained from the expert evaluation confirm that Artefact 3 is a cost-effective framework for organisations.
Evidence Against
There is no reference or evidence found that refutes the stated Hypothesis 3.
Verdict => Accepted
Solution objectives described in Chapter 2, an ADSRM approach applied in Chapter 3, framework principles and FAIR model described in Chapter 3, FAIR model integrated into Chapter 4, and noted positive feedback received from the experts in Chapter 5 provides sufficient evidence that Hypothesis 3 cannot be rejected.

6.3 ANSWERS TO RESEARCH QUESTION

In Chapter 3, Section 3.2.1, the primary research question was articulated as follows: "**What framework aligns the current ISO/IEC 27050 standard with the ISO security risk evaluation framework in a cost-effective way?**"

The relation between the results of the previous chapters with the answers provided for the research sub-questions in Section 6.1 and hypotheses testing in Section 6.2 is summarised in Figure 6.2 to establish the research finding.

First, to answer Sub-Question 1, it has been found that the current ISO/IEC 27050 standard does not have any sort of security risk management framework. At present, the eDiscovery guidelines ignore security risks and are populated by technical assistance for discovery. The use of these guidelines without a risk framework puts the users and the information at risk of disclosure and damage. Hence, the ISO/IEC 27050 standard has no security provisions for information protection.

Second, in Sub-Question 2, the proposed security risk management framework has been constructed using the strawman (theory) method explained in Section 3.5.2.4. This

method started with designing the intended framework from theory, developing three scenarios, testing the framework, and then doing the first feedback iteration. Based on the feedback, the framework has been improved and then communicated to selected experts for their opinion. Next, the expert feedback has been further analysed through NVivo data analysis. Then, the final version of the framework has been improved based on the feedback received from the experts.

Third, in regards to Sub-Question 3, integrating the new Artefact 3 with the current ISO/IEC 27050 standard has been achieved through two integration dimensions: overall process dimension through the mapping between the eDiscovery components and the security risk management components; and risk estimation activities dimension using the new modified version of FAIR model.

After applying adjustments to the original framework, it is evident that this research has filled the gap by designing a new effective security risk management framework. The added value of the proposed framework model has shown a shift from a requirements standard control approach towards an action-oriented and referenced approach.

In conclusion, the results obtained from the expert evaluation confirm that the developed Artefact 3 is a cost-effective and fit-for-purpose framework for organisations that can be used to evaluate the ability of an organisation to meet the objectives of security risk management; and therefore, improve the risk identification process in the eDiscovery field when using the ISO/IEC 27050 standard.

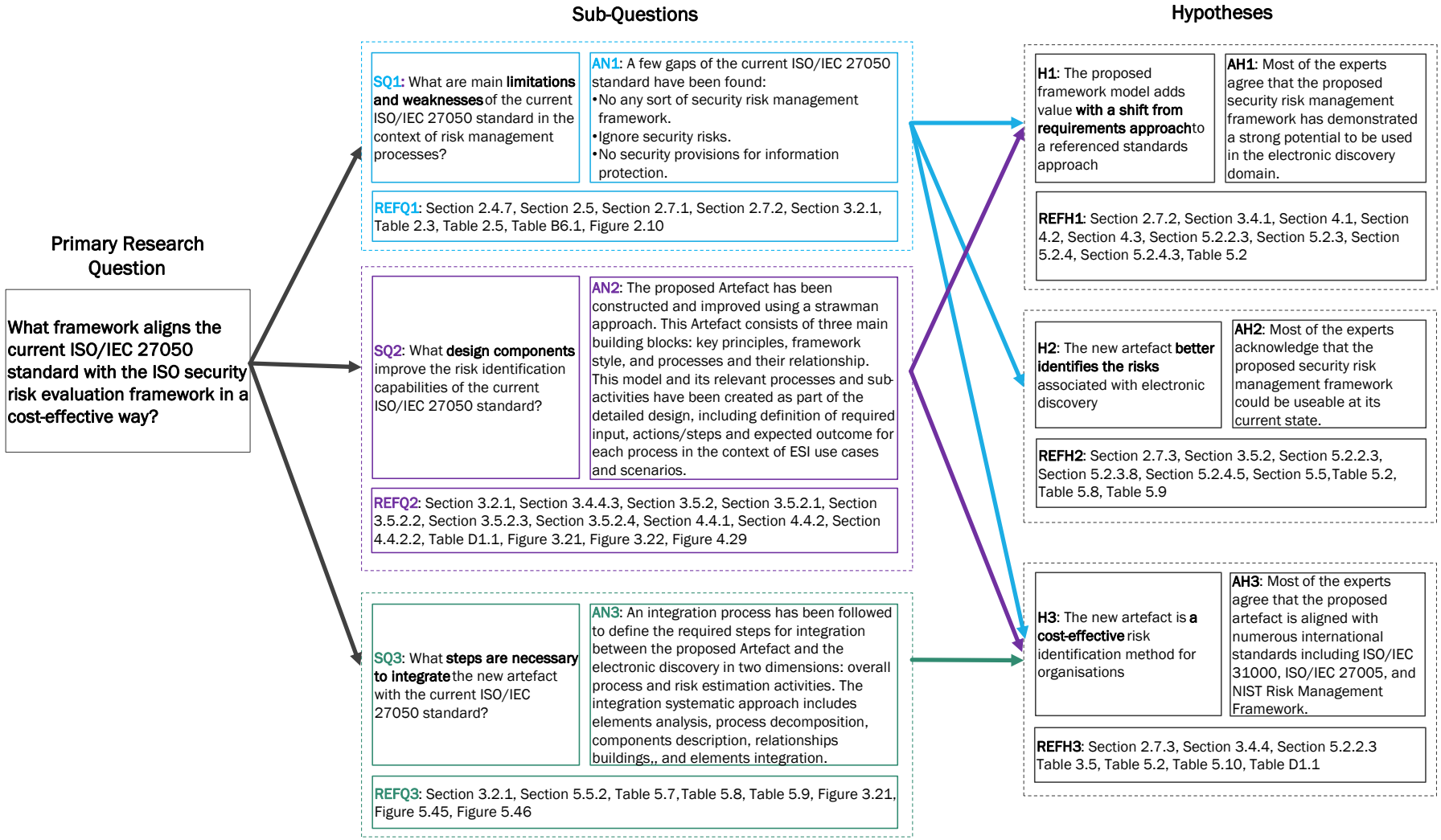


Figure 6.2: Summary of Answers to Research Question, Sub-Questions, and Hypotheses

6.4 DISCUSSION

This research investigated a well-defined security risk management framework applied to the ISO/IEC 27050 standard to provide mechanisms that allow organsiations to evaluate their ESI security risk. Although the ISO/IEC 27050 standard helps in identifying the risks associated with eDiscovery and then providing a basic mitigation plan, it does not provide a detailed description of how to identify risks and manage them. Instead, it provides high-level requirements for the whole ESI investigation process. A risk management reference model was developed to assess the current state of the ISO/IEC 27050 standard in terms of its capabilities to manage security risk. The assessment indicated that 50% of the risk management reference model capability was missing which represents a considerable gap. The researcher compared five selected risk management frameworks: ISO/IEC 31000, ISO/IEC 27005, NIST 800-37, ENISA, and The Risk IT with risk-related elements found in the literature, then incorporated different aspects from each into a new risk-based security framework. There was insufficient guidance for effectively managing risks associated with ESI, particularly in addressing specific challenges such as aligning information security with ESI risk management alignment. Consequently, this arose necessary to identify a solution that could bridge this gap and provide a comprehensive approach to addressing these challenges.

In this research, a conceptual model has been constructed using an ADSRM approach (i.e., a researcher's selection of methods) to evaluate the ability of an organisation to meet the objectives of security risk management when using the ISO/IEC 27050 standard. This model comprises three main building blocks: a set of principles, framework style, and processes, and their relationship to managing, measuring, and controlling all aspects of security risk in the eDiscovery domain. A modified version of the FAIR model was adapted into the framework as a risk estimation engine to perform data/estimates for higher levels of abstraction. A mapping between the proposed security risk management framework concepts and its components has been presented using an ArchiMate 3.1 metamodel. Architects and designers can utilise this metamodel to construct models of risk-related activities, enabling the creation of multiple perspectives from motivation, strategy, and business standpoints. These models offer a comprehensive framework for capturing and visualizing risk-related information, facilitating a holistic understanding of risk across various dimensions.

The set of guidelines in the ISO/IEC 31000 and ISO/IEC 27005 frameworks and others in the literature, strengthened the framework consistency. Therefore, the researcher can argue that this framework has a strong theoretical foundation. Moreover, a combination of three testing scenarios and ten experts' feedback was used to improve the proposed Artefact 2 and prove its added value to organisations. A selected group of experts evaluated the proposed framework against eight distinct evaluation criteria using a qualitative method. These criteria addressed various characteristics, including the efficacy of the proposed artefact for eDiscovery risk management, clarity of its components, its usefulness to the workplace, its alignment with international security risk management standards, its usability and implementation, the possibility to improve its robustness, the necessity to improve its current capabilities, and its applicability to further modifications. The expert evaluation provided different points of view and perceptions that assisted the relevance of the proposed Artefact 2 and validation.

The expert's evaluation results showed that most of the experts believe the proposed Artefact 2 has demonstrated a strong potential to be used in the eDiscovery domain if some adjustments/corrections are enacted to its specific components. They also indicated that the proposed artefact would be useful for their workplace. Furthermore, most of the experts agree that the proposed artefact is aligned with numerous international standards because it consists of all major components of a risk management framework and follows the PDCA model.

A strong framework is key for organisations to manage risk. Drawing upon the existing practices and literature, this research has presented a comprehensive framework for risk identification and risk management in the eDiscovery domain. By incorporating broader perspectives and insights, this framework encourages organisations to adopt a more comprehensive approach to addressing security risks in the eDiscovery context. However, like any other framework, the proposal has some limitations due to its structure and applicability. These limitations present challenges in different areas, including generalisation, providing a customisable security controls catalogue, using pre-defined risk metrics, plugging internal audit activities in, and covering and aligning with all NIST framework dimensions (i.e., identity, protect, detect, respond, and recover), and finally implementing the framework to make it more tangible, demonstrable, and verifiable.

6.5 RESEARCH CONTRIBUTION

DSR endeavours to develop ground-breaking artefacts to tackle complex, and practical issues, subsequently generating design knowledge (Akoka et al., 2022). The primary objective of DSR lies in constructing and evaluating tangible solutions. The artefact pertains to an artificial creation constructed by humans. It is imperative for this artefact to enhance current problem-solving approaches or potentially provide a pioneering solution to a crucial problem (Hevner & Chatterjee, 2010).

In this research, an abstract artefact (e.g., a framework in the context of this research) has been constructed as a general concept (contribution), followed by a study of ESI use cases (knowledge). The abstract artefact created through DSR is implemented in practical examples, such as real-life scenarios., to evaluate its effectiveness. Feedback is then sought from relevant experts to evaluate and improve the artefact's performance. Moreover, the abstract artefact could be converted into a material reality in the form of a tool.

This research attempts to address the current gaps in the ISO/IEC 27050 standard and make important contributions to knowledge. The main contribution of this study is the creation of a clearly defined framework that enables organisations to identify and address security risks specific to the eDiscovery domain.

The research contributes to the body of knowledge and is presented in two main aspects: theory and practice as detailed in the subsections below.

6.5.1 Contribution to Theory

An adaptive research approach (i.e., ADSRM) was selected based on the combinations of both DSRM and DSRP methodologies with a few adjustments. This adaptive methodology provides a state-of-art process to define the problem statement, design a risk identification framework artefact, produce a new solution, evaluate and improve the artefact, and communicate research findings.

The researcher took a theoretical artefact (strawman framework Design 1) developed from phases 1, 2, and 3 in the Peffers' model and then entered into Phase 4 where "How to knowledge" was used to test the relevance of the framework. To achieve this, three scenarios were taken from the literature and the framework was applied to mitigate risks in the eDiscovery processes.

A DS investigation was chosen as an exploratory methodology where an artefact was produced, reviewed, evaluated, and improved. The proposed artefact was tested

through three different scenarios. Furthermore, it was evaluated with the data collection method using experts' feedback. Defined research questions with three supporting sub-questions were answered. Proposed hypotheses were validated by employing the quasi-judicial method, which involves analysing the qualitative data and applying a rational argument to interpret the findings.

The research journey concludes with the presentation of a comprehensive PhD thesis, encapsulating key elements, including the definition of the problem, a thorough review of the existing literature, the development of hypotheses, the identification of data requirements, data analysis procedures, the resulting findings, an in-depth discussion, and a conclusive summary. This thesis serves as a comprehensive documentation of the primary outcomes derived from the research endeavour. Furthermore, the intermediate data will be published in the form of a Journal articles and Conference papers upon finalising this thesis.

6.5.2 Contribution to Electronic Discovery Investigation

The mapping between the developed security risk management framework and the eDiscovery lifecycle plays a major contribution to this research. This is because the proposed artefact offers a new perceptive that provides a well-structured approach to risk identification and management in an ESI investigation.

In practice, eDiscovery investigators in government agencies and legal offices can use the proposed framework to perform investigations, evidence acquisition, and handling ESI more safely and consistently. The eDiscovery investigators follow rules and steps to identify and preserve relevant ESI when an investigation is initiated to meet various investigation requirements. The security risk is controlled and managed using the proposed framework that is tailored to the eDiscovery process. The proposed framework was evaluated by a selected group of experts as being a useful tool. The data collected by the expert feedback validated the fact that the experts found the proposed artefact valuable for risk identification and management in the eDiscovery domain.

The developed testing scenarios simulated real-life situations and reinforced the concepts and methods that have been introduced in this research. These scenarios covered three different sectors as described in Table 6.4.

Table 6.4: Summary of Scenarios Testing

Sector	Scenario	Potential Risk
Energy	The process of searching, locating, and securing electronic data to use it as evidence in a legal case.	There is a potential risk when users access and share sensitive information stored on emails, file servers and databases. Support is required to manage a large amount of stored information, implement legal holds on data, and meet regulatory compliance obligations for litigation efforts.
IT	The data leakage issue that organisations face when they store the IP of third parties in multiple locations.	There is a potential risk when organisations move their data and systems to the cloud. Using a SaaS-based eDiscovery solution introduces risks from two key perspectives: data sovereignty in the cloud and discovery technology implemented in the cloud. On the other hand, when data is split between on-premises and cloud environments, transferring data between them increases risks.
Health Care	The implication of inconsistent medical records from a risk perceptive is when data moves between physicians, hospitals, clinics, and patients.	External threats could cause data inconsistency in the EMR platform (e.g., manipulation attacks). Incomplete data poses a potential risk, leading to higher reimbursements and lower staff-to-patient ratios. Consequently, clinicians bear the burden of heavy workloads. Staff often make inconsistent documentation because they focus on treating the patient, so documentation becomes a less priority.

Figure 6.3 illustrates the ALE that occurred most frequently in the simulated results of the scenarios above for three different threat communities: Insider, Cyber Criminals, and Organised Crime Groups. These values are set within the Significance scale according to Table 4.16 presented previously in Chapter 4. Moreover, the scale represented one possible set of ranges to characterise the loss. Organisational loss capacity and tolerances were reflected in the range encompassed by the scales. This range was determined by comparing expected outcomes to the best and worst-case scenarios. This emphasises the constraint of ordinal matrices linked to numeric ranges in accurately representing the entire spectrum of potential outcomes.

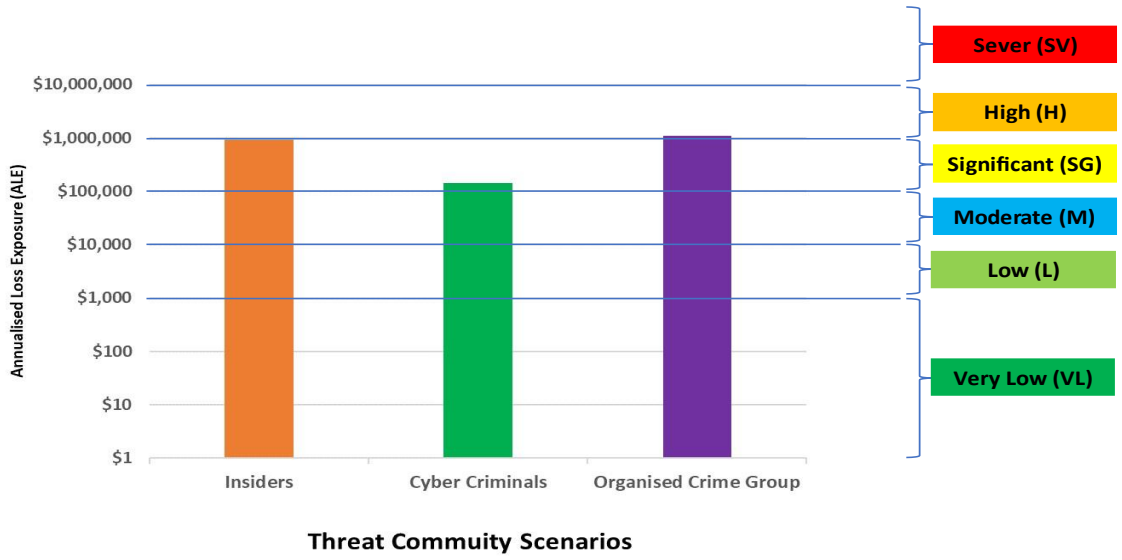


Figure 6.3: Expressing Quantitative Risk in Impact Thresholds

The first scenario focused on insiders maliciously accessing an eDiscovery platform and misusing sensitive information using privileged access capabilities. The risk analyst is tasked to analyse the risk associated with privileged insiders impacting the confidentiality of the eDiscovery platform via malicious access. Since eDiscovery involves the identification, gathering, analysis, and transfer of information (e.g., documents and email) that be used in the legal process for lawsuits, these activities can be limited to employees only (privileged insiders and non-privileged insiders). The data obtained for eDiscovery possesses a distinct quality as it comprises precise information that is requested by Legal Counsel to address a legal matter. Trusted insiders may destroy, alter, or steal sensitive information. If any employee with access misuses their rights, privileges, and access, they can present a substantial insider threat to the organisation. Unrestricted disclosure of information can cause various damages to organisations. To prevent unauthorised privileged insiders from accessing and intentionally or unintentionally releasing this type of data, a set of security measures is necessary. The calculated ALE (Most Likely) in the case of insiders accessing sensitive information was $930,400 as illustrated in Figure 6.3. This value is set at the edge of the Significance scale.

The second scenario evaluated the risk of cyber criminals maliciously accessing eCommerce databases and misusing sensitive information through phishing campaign capabilities. The organisation requested their risk analyst to analyse the risk associated with cyber criminals impacting the confidentiality of third-party IP in the eCommerce

database via a phishing attack. The calculated ALE (Most Likely) in the case of cyber criminals accessing sensitive information was $142,000 as depicted in Figure 6.3. This value is set within the Significance scale.

The last scenario tested the capability of an organised crime group to maliciously access the EMR platform and then perform an unauthorised modification to personal information using a data manipulation technique. The assigned risk analyst needed to analyse the risk associated with organised crime groups impacting the integrity of patient information stored in the EMR platform via a ransomware attack. The calculated ALE (Most Likely) in the case of an organised crime group performing an authorised modification was $1,100,000 as exhibited in Figure 6.3. This value exceeded the Significance scale range, reaching the beginning of the High scale.

6.6 CONCLUSION

In this chapter, the primary research question, three sub-questions, and three hypotheses have been articulated.

It was concluded that the current ISO/IEC 27050 standard has no security provisions for information protection (Sub-Question 1). The Strawman method has been used to construct the proposed security risk management framework (Sub-Question 2). Integrating the new Artefact 3 with the current ISO/IEC 27050 standard has been achieved through two integration dimensions: overall process dimension through the mapping between the eDiscovery components and the security risk management components; and risk estimation activities dimension using the new modified version of the FAIR model (Sub-Question 3). The outcomes derived from the expert evaluation confirmed that the developed Artefact 3 is a cost-effective (Hypothesis 3) and fit-for-purpose framework for organisations (Hypothesis 1) that can be used to evaluate the ability of an organisation to meet the objectives of security risk management; and therefore, improve the risk identification process in the eDiscovery field when using the ISO/IEC 27050 standard (Hypothesis 2).

The research makes a valuable contribution to the current body of knowledge in both theoretical and practical domains. In theory, the researcher takes a strawman method and entered into the “How to knowledge” phase to test the relevance of the framework. To achieve this, three scenarios have been developed and then the framework has been applied to mitigate risks in the eDiscovery processes. In practice, eDiscovery investigators in government agencies and legal offices can use the proposed framework

to perform investigations, evidence acquisition, and handling ESI in a more controlled manner. The security risk is controlled and managed using the proposed framework that is tailored to the eDiscovery process.

Finally, this chapter provides the outcomes of this research in terms of results, contributions, and limitations for Chapter 7 to complete. Thus, Chapter 7 provides suggestions for further research arising from this study. Additionally, Chapter 7 restates the purpose of the research and then summarises what has been found concerning the primary research question and its sub-questions.

Chapter 7: Conclusion

7.0 INTRODUCTION

Figure 7.1 shows the summary of the thesis structure based on the proposed research methodology. The dashed lines show the roadmap for Chapter 6 and Chapter 7 which is Phase 6 (Artefact Results Demonstration).

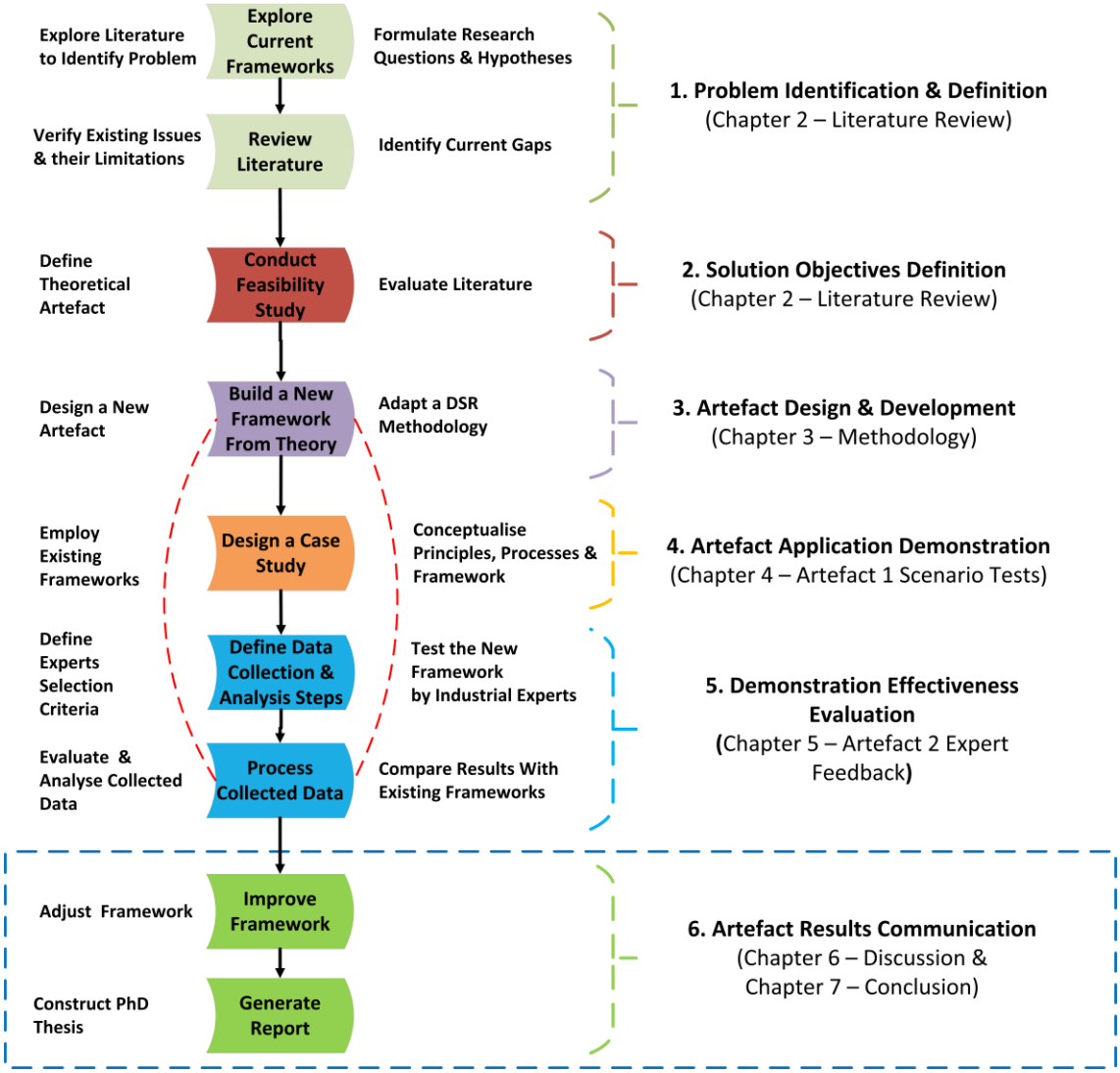


Figure 7.1: Chapter 7 Roadmap

This study focused on finding a solution to ensure the eDiscovery process is followed securely. The research aimed to develop a well-defined security risk management framework applied to the ISO/IEC 27050 standard with mechanisms that allow organsiations to evaluate their ESI security risk. The proposed framework has been integrated into the eDiscovery domain by interlinking the various components of both security risk management practice and the eDiscovery process.

In this chapter, a summary of all thesis chapters is restated along with future research work suggestions. This chapter is organised as follows. Section 7.1 provides a summary of what was found about the primary research question and its associated sub-questions. It summarises all the key points of the thesis from Chapter 2 to Chapter 6. The research contribution to the body of knowledge is restated in Section 7.2. Section 7.3 explains the limitations of this study. Section 7.4 concludes the whole thesis with a set of suggestions for future research.

7.1 RESEARCH SUMMARY

Organisations face challenges to assess their potential security risk when establishing the eDiscovery process. The problem addressed in this research comes from the literature review process which has identified a gap that exists within the ISO/IEC 27050 standard. The findings of this research demonstrated that the ISO/IEC 27050 standard offers the requirements and guidance for the discovery of ESI or data by one or multiple parties engaged in investigations, litigation, or similar proceedings. However, there were no security provisions for information protection. In other words, the current ISO/IEC 27050 standard does not have any sort of security risk framework.

The eDiscovery is a systematic process that involves seven main phases: identification, preservation, collection, processing, reviewing, analysis, and production.

The research investigation has led to the following primary research question: "**What framework aligns the current ISO/IEC 27050 standard with the ISO security risk evaluation framework in a cost-effective way?**" with its associated three sub-questions: *SQ1) What are the main limitations and weaknesses of the current ISO/IEC 27050 standard in the context of risk management processes? SQ2) What design components improve the risk identification capabilities of the current ISO/IEC 27050 standard? SQ3) What steps are necessary to integrate the new artefact with the current ISO/IEC 27050 standard?*

ADSRM approach was selected to answer the primary research question through expert feedback of three hypotheses: *H_1) the proposed framework model adds value with a shift from requirements approach to a referenced standards approach, H_2) the new artefact better identifies the risks associated with electronic discovery, H_3) and the new artefact is a cost-effective risk identification method for organisations.*

A risk management reference framework was developed to assess the current state of the ISO/IEC 27050 standard in terms of its capabilities to manage security risk. The

assessment found that 50% of the risk management reference framework capabilities were missing as described in Table 7.1.

Table 7.1: Missing Activities in the ISO/IEC 27050 Standard

Phase	Missing Activities
Phase 1 – Context Establishment	1.3 Define risk management criteria (evaluation, impact, acceptance) 1.4 Define scope and boundaries
Phase 2 – Risk Identification	2.1 Decide on risk analysis method (Qualitative or Quantitative) 2.6 Identify vulnerability 2.8 Identify incident scenarios with their consequences
Phase 3 – Risk Estimation	3.1 Assess threat likelihood of occurrence (probability) 3.2 Assess vulnerability 3.3 Assess existing controls implementation status 3.4 Assess business impact 3.5 Determine the risk level
Phase 4 – Risk Evaluation and Treatment	4.2 Prioritise risk 4.3 Recommend a risk treatment plan

The entire Phase 3 (risk estimation) was missing from the ISO/IEC 27050 and most of Phase 4 activities (risk evaluation and treatment). Additionally, two activities of Phase 1 (context establishment) and Phase 2 (risk identification) were not covered.

The researcher compared five selected risk management frameworks: ISO/IEC 31000, ISO/IEC 27005, NIST 800-37, ENISA, and The Risk IT, with risk-related elements found in the literature, and incorporated different aspects into a Strawman Artefact 1.

The proposed security risk management framework has been constructed using the Strawman method. This method started with building the intended framework from theory, developing three scenarios, testing the framework, and then getting the first feedback iteration. Based on the first feedback, the framework has been improved (Artefact 2) and then communicated to selected experts for their opinion. Next, the expert feedback has been further analysed through NVivo data analysis. Subsequently, the framework's final version has been improved (Artefact 3) by incorporating the feedback received from the experts during the second round of evaluations.

A DS investigation has been used as an empirical methodology to produce, review, and evaluate the desired Artefact, and re-design it if required. Then, the proposed

Artefact underwent evaluation using a data collection method. The defined hypotheses were tested by analysing qualitative data through a quasi-judicial approach, utilising rational arguments to interpret the data.

The structure of the proposed framework consists of three building blocks: principles, framework style, processes, and their relationship. Ten overarching principles guide the proposed framework: protection, integration, systematic, alignment, responsibility, capability, quantitative, human behaviour, conformance, and continual improvement. The proposed framework has five core components: establish, identify, estimate, evaluation and treat, and monitor and improve. In addition to that, it presents five key outputs: risk criteria, risk analysis method, risk level, risk treatment plan, and process improvement. Each component represents a distinct process phase with a set of activities that forms the overall security risk management framework. The five process phases are organised into three assessment states: pre-assessment (Context Establishment), during assessment (Risk Identification, Risk Estimation, and Risk Evaluation & Treatment), and post-assessment (Monitoring & Improvement).

The proposed security risk management framework incorporates a versatile qualitative FAIR model approach, which is seamlessly integrated within it. The estimation of risk using the FAIR model was conducted by utilising data and estimates at higher levels of abstraction within the given context. This integration enabled risk analysts to choose the most suitable level of analysis, taking into account factors such as time, data availability, complexity, and the significance of the scenario. Furthermore, the researcher derived a set of formulas that present the functional relationships between variables (risk factors in the FAIR model), either statically or probabilistically, capturing the dependencies between a factor and its sub-factors.

Ten selected experts have been contacted to participate in evaluating the proposed artefact. The number of experts participating in the research was chosen based on the literature discussed to ensure that both data the collection and analysis processes are manageable. The expert feedback was collected and then assessed and analysed against eight criteria of the proposed artefact: efficacy, clarity, usefulness, alignment, usability, robustness, improvability, and completeness. The research evaluation showed that 80% of the experts believed that the proposed artefact would be effective for eDiscovery risk management as well as being aligned with the international security risk management standards. Two-thirds of them indicated the defined components of the proposed artefact are clear and relevant and they acknowledged that it could be useable in its current state.

Most of the experts indicated that the proposed artefact would be useful for their workplace. Almost 80% of the experts believed that the proposed artefact would improve risk management. 75% of the experts believed that some adjustments/corrections should be enacted to specific components of the proposed artefact.

The proposed security risk management framework was resolved and mapped using ArchiMate 3.1. This has provided a comprehensive architecture with graphical notation, relationships, and metamodel following three architecture layers: motivation, strategy, and business.

The overall results obtained from the expert evaluation confirmed that the developed Artefact 3 is a cost-effective and fit-for-purpose framework for organisations that can be used to evaluate the ability of an organisation to meet the objectives of security risk management; and thus, improve the risk identification process in the eDiscovery field when using the ISO/IEC 27050 standard.

The researcher concluded that the proposed security risk management framework can enable organisations to establish a defensible process to simultaneously reduce potential security risk while also increasing the capability and maturity level of the eDiscovery process. Moreover, by establishing a secure eDiscovery process, organisations can not only save money but also significantly improve their compliance.

7.2 RESEARCH CONTRIBUTIONS

The proposed framework provides guidelines on establishing the context, communicating, and addressing risk. However, it lacks an approach for assessing the true nature and impact of risk (referred to as the risk assessment approach). In contrast, the FAIR model provides an approach specifically designed for determining the nature and impact of actual risk. By integrating the proposed framework into the FAIR, it becomes possible to establish a comprehensive framework and approach for estimating and analysing risks in the eDiscovery process (Group, 2010).

In this research, an abstract artefact (e.g., a framework in the context of this research) has been produced as a general concept (contribution), followed by a study of ESI use cases (knowledge). A DS has been selected to guide this research by using a Strawman theoretical construct.

The proposed framework was constructed and improved through different activities, including establishing a framework from theory, producing three scenarios,

testing those scenarios, improving Artefact 1, and evaluating Artefact 2 by a group of selected experts until realising Artefact 3.

To demonstrate the proposed security risk management framework, this study presents three disparate scenarios of an Energy Provider, IT Service Provider, and Health Care Service Provider respectively. These scenarios have reinforced the concepts and methods that have been introduced in this study. First, there is a brief description of a scenario, followed by a list of requirements for each scenario. Second, each scenario was tested using the first Artefact of the proposed framework. Thirdly, the final results were examined to correct errors and omit any wrong data. The scenarios above have identified three potential risks as illustrated in Figure 7.2.

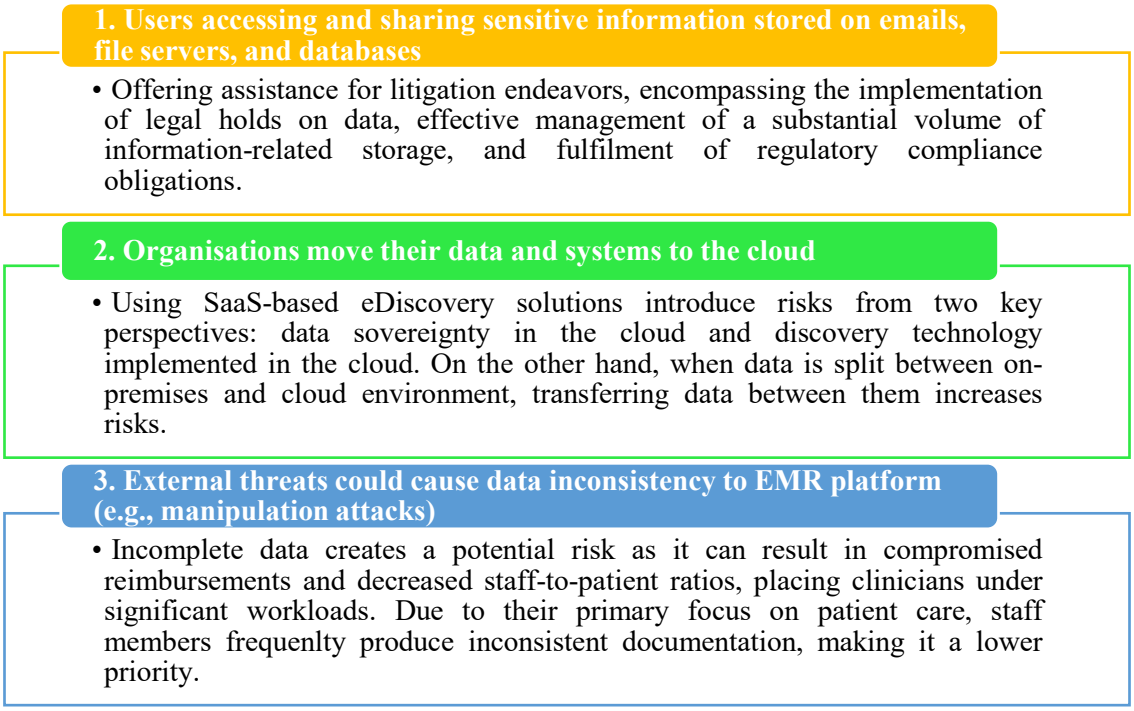


Figure 7.2: Summary of Potential Risks

Overall, the assessment of the proposed framework model's value involved industry-specific usability testing. Valuable insights regarding its practical worth were obtained through expert feedback on Artefact 2. Following a thorough analysis of this feedback, essential adjustments were made to Artefact 2 to bring it in closer alignment with these insights. Artefact 3 is now awaits piloting real-world testing in diverse settings, with a particular emphasis on evaluating its broader practical applicability.

7.3 RESEARCH LIMITATIONS

In this research, a combination of three testing scenarios and ten experts' feedback has contributed to the overall artefact improvement. The expert evaluation has provided different points of view and perceptions that assisted the accuracy of the proposed artefact and validation.

However, like any other framework, the proposal has limitations due to its structure and applicability. These limitations pose challenges in various areas such as generalisation, creating a customisable security controls catalogue, utilising predefined risk metrics, integrating internal audit activities into the proposed framework, aligning with all NIST framework dimensions (i.e., identifying, protecting, detecting, responding, and recovering), and implementing it to achieve more tangible, demonstrable, and verifiable results. In other words, implementation of the proposed artefact poses a challenge for this study, demanding additional resources and the adoption for a specific methodology, as discussed by Nunamaker et al. (1990), which addresses system development methodologies.

The research did not address aspects of risk management beyond risk assessment, monitoring and improvement; and it is limited to activities only related to how to design and conduct a risk assessment, including risk establishment, risk assessment (identification, analysis), risk calculation, risk treatment, risk acceptance, and capability improvement. The risk communication and consultation phase has not been covered in the context of this study.

In hindsight, the researcher employeed the DSRM to create a practical solution to a specific problem. This necessitated a strong technical background to effectively implement DSRM, given that it assumes a certain level of expertise. However, the DSRM, while offering a high-level framework, lacks detailed step-by-step guidance. Conseqently, the reseacher had to adapt the methodology to the specific research context, a challenging task due to the researcher's newness to the methodology. Furthermore, the DSRM provides less detailed guidance on data collection and analysis compared to some other research methodologies. Therefore, the researchers had to incorporate additional methods to effectively address these aspects such as the NVivo tool to ensure robust data collection and analysis.

On the other hand, the researcher would extend the research by incorporating a comparative analysis of various risk quantification methods, not limited to the FAIR model, including both quantitative and qualitative approaches, as well as different risk

modeling tools beyond Monte Carlo. This approach may offer a more comprehensive understanding of the strengths and weaknesses of each method and tool, leading to a better outcome.

Lastly, but significantly, due to the high level of subjectivity inherent in the data collection used in this research, limitations persist throughout all stages. As a result, it remains crucial to continually enhance the industry's usability and efficiency of the proposed artefact based on feedback from experts. This iterative process of refinement ensures that the seurity risk management framework can adapt and evolve to address the inherent challenges associated with subjective data collection, thus maintaining its relevance and effectiveness over time.

7.4 RECOMMENDATIONS FOR FUTURE RESEARCH

The research has determined that the proposed artefact is viewed favourably and holds the promise of effectively handling risks in the eDiscovery process. It has been observed that the number of experts participating in the research evaluation is relatively small. In the future, this research should be evaluated using a larger number of experts. This would improve the feedback quality and provide more visibility in terms of the usability and fitness of the proposed artefact.

During the expert feedback activities, the experts provided some suggestions to improve the overall quality of the proposed artefact (as described in Table 5.6). Some suggestions have not been applied because they are not within the established scope of this study. Thus, further research is needed to consider them in a new version of the framework.

Like any other framework, the proposed framework has some limitations due to its structure and applicability. These restrictions present difficulties in multiple domains, including the ability to apply knowledge universally, develop a flexible catalogue of security controls, utilise predetermined risk measurements, incorporate internal audit activities within the proposed framework, align with all aspects of the NIST framework, and successfully implementing it to attain concrete, provable, and measurable outcomes.

In future work, the researcher could define risk metrics and risk selection methods; and then add new components to the Risk Monitoring & Improvement process. This would ensure that the proposed framework produces comparable and reproducible results. Additionally, by introducing internal audit activities, the proposed framework will ensure

the identification of nonconformities and the subsequent creation of corrective action and improvement plans.

In light of the utilisation of the FAIR model within the proposed security risk management framework, there remain a few questions that require more investigation in the future. For example, does the FAIR model provide a framework to address inquiries like what level of risk does X pose? How much risk does an organisation carry? How does risk change in various scenarios? Which risk management options are most efficient in terms of cost?

Nevertheless, there are several disadvantages to quantifying risk using the FAIR model, including its time and cost-intensive nature, the need for a thorough comprehension of the FAIR model ontology, manual data collection, and the involvement of scenario-specific risk analysts or experts for inputs. There may be other alternative models that perform similar capabilities but these need researching.

Another aspect is that the FAIR model provides all the technical details of information risk with a flowchart of facts (i.e., taxonomy). But, without prior exposure to the FAIR model, it may be challenging to navigate the analysis required to make functional and useful analysis inputs. Facilitation processes that are easy to use and learn are needed and required further research. Also, with all its complexity, it will be challenging for risk analysts to calculate an ALE using the FAIR model without software assistance (e.g., RiskLens and Balbix). The software has been specifically created and designed to make life easier for the implementation of the FAIR model but it requires testing and integration into the proposed framework.

References

Agrawal, V. (2015). *A Comparative Study on Information Security Risk Analysis Methods*. https://doi.org/10.17706/jcp.12.1.57-67

Akoka, J., Comyn-Wattiau, I., Prat, N., & Storey, V. C. (2022, 2022/11/13/). Knowledge contributions in design science research: Paths of knowledge types. *Decision Support Systems*, 113898. https://doi.org/https://doi.org/10.1016/j.dss.2022.113898

Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger. In H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, & H. Al-Khateeb (Eds.), *Blockchain and Clinical Trial: Securing Patient Data* (pp. 149-168). Springer International Publishing. https://doi.org/10.1007/978-3-030-11289-9_7

Alam, M. K. (2021). A systematic qualitative case study: questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management: An International Journal, 16*(1), 1-31. https://doi.org/10.1108/QROM-09-2019-1825

Almeida, R., Teixeira José, M., Mira da Silva, M., & Faroleiro, P. (2019). A conceptual model for enterprise risk management. *Journal of Enterprise Information Management, 32*(5), 843-868. https://doi.org/10.1108/JEIM-05-2018-0097

Anttila, J., & Kajava, J. (2010, 15-18 Feb. 2010). Challenging IS and ISM Standardization for Business Benefits. 2010 International Conference on Availability, Reliability and Security,

Archi. (2022). *Archi Modelling Tool: Archi User Guide Version 5.0.2*. Archi. https://www.archimatetool.com/downloads/archi/Archi%20User%20Guide.pdf

Arshad, H., Omlara, E., Abiodun, I. O., & Aminu, A. (2020, 2020/10/01/). A semi-automated forensic investigation model for online social networks. *Computers & Security, 97*, 101946. https://doi.org/https://doi.org/10.1016/j.cose.2020.101946

Barateiro, J., Antunes, G., & Borbinha, J. (2012, 4-7 Jan. 2012). Manage Risks through the Enterprise Architecture. 2012 45th Hawaii International Conference on System Sciences,

Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects: A Guide for Students in Computer Science and Information Systems*. https://doi.org/10.1007/978-1-84800-009-4

Bhatia, S., & Malhotra, J. (2020, 2020//). CFRF: Cloud Forensic Readiness Framework – A Dependable Framework for Forensic Readiness in Cloud Computing Environment. Innovative Data Communication Technologies and Application, Cham.

Blind, K., & Gauch, S. (2008, 2008/08/01/). Trends in ICT standards: The relationship between European standardisation bodies and standards consortia. *Telecommunications Policy, 32*(7), 503-513. https://doi.org/https://doi.org/10.1016/j.telpol.2008.05.004

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016, 2016/02/01/). A review of cyber security risk assessment methods for

SCADA systems. *Computers & Security, 56*, 1-27. https://doi.org/https://doi.org/10.1016/j.cose.2015.09.009

Collis, J., & Hussey, R. (2021). *Business Research : A Practical Guide for Students*. Bloomsbury Publishing Plc. http://ebookcentral.proquest.com/lib/aut/detail.action?docID=6526176

de Vries, H. J., Jakobs, K., Egyedi, T., Eto, M., Fertig, S., Kanevskaia, O., Klintner, L., Koch, C., Mijatovic, I., Mirtsch, M., Morone, P., Orviska, M., Riillo, C., & Scaramuzzino, G. (2018, 01/01). Standardization: Towards an Agenda for Research. *International Journal of Standardization Research, 16*, 52-59. https://doi.org/10.4018/IJSR.2018010104

de Vries, H. J., & Veurink, J. (2017, 01/01). Cost-Benefit Analysis of Participation in Standardization: Developing a Calculation Tool. *International Journal of Standardization Research, 15*, 1-15. https://doi.org/10.4018/IJSR.2017010101

Dresch, A., Lacerda, D., & Jr, J. (2014). *Design Science Research: A Method for Science and Technology Advancement*. https://doi.org/10.1007/978-3-319-07374-3

ENISA. (2006). Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools. *The European Union Agency for Cybersecurity (ENISA)*.

ENISA. (2007). Risk Management and IT Security for Micro and Small Businesses. *The European Union Agency for Cybersecurity (ENISA)*.

Freund, J., & Jones, J. (2014). *Measuring and Managing Information Risk: A FAIR Approach*. Butterworth-Heinemann.

Gallego, D., & Bueno, S. (2014, 2014/10/21). Exploring the application of the Delphi method as a forecasting tool in Information Systems and Technologies research. *Technology Analysis & Strategic Management, 26*(9), 987-999. https://doi.org/10.1080/09537325.2014.941348

Group, T. O. (2010). *FAIR - ISO/IEC 27005 Cookbook*. The Open Group Library. https://publications.opengroup.org/c103

Group, T. O. (2013). *Risk Analysis (O-RA)*. The Open Group Library. https://publications.opengroup.org/c13g

Group, T. O. (2019). *ArchiMate 3.1 Specification*. The Open Group Library. https://pubs.opengroup.org/architecture/archimate31-doc/

Guest, G., Bunce, A., & Johnson, L. (2006, 2006/02/01). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods, 18*(1), 59-82. https://doi.org/10.1177/1525822X05279903

Hatto, P. (2010). *Standards and Standardisation Handbook*. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/db289e47-140b-11eb-b57e-01aa75ed71a1

Heikkila, F. M. (2008). E-Discovery: Identifying and Mitigating Security Risks during Litigation. *IT Professional, 10*(4), 20-25. https://doi.org/10.1109/MITP.2008.67

Hevner, A., & Chatterjee. (2010). *Design Research in Information Systems: Theory and Practice* (Vol. 22). https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A., R, A., March, S., T, S., Park, Park, J., Ram, & Sudha. (2004, 03/01). Design Science in Information Systems Research. *Management Information Systems Quarterly, 28*, 75.

Hoel, T., & Chen, W. (2018, 01/01). Interaction Between Standardisation and Research: A Case Study. *International Journal of Standardization Research, 16*, 22-38. https://doi.org/10.4018/IJSR.2018010102

ISACA. (2009a). The Risk IT Framework: Principles Process, Details Management, Guidelines and Maturity Models. *Information Systems Audit and Control Association (ISACA)*.

ISACA. (2009b). *The Risk IT Partitioner Guide*. ISACA.

ISO. (2016). Information technology — Governance of digital forensic risk framework (ISO/IEC 30121:2015). *International Organization for Standardization (ISO)*.

ISO. (2018a). ISO/IEC 27050-1:2019, Information Technology - Electronic Discovery, Part 1: Overview and concepts. *International Organization for Standardization (ISO)*.

ISO. (2018b). ISO/IEC 27050-2:2018, Information Technology - Electronic Discovery, Part 2: Guidance for Governance and Management of Electronic Discovery. *International Organization for Standardization (ISO)*.

ISO. (2018c). ISO/IEC 31000:2018, Risk Management - Guidelines. *International Organization for Standardization (ISO)*.

ISO. (2019). IEC 31010:2019, Risk Management – Risk Assessment Techniques *International Organization for Standardization (ISO)*.

ISO. (2020a). ISO/IEC 27050-3:2020, Information Technology - Electronic Discovery, Part 3: Code of Practice for Electronic Discovery. *International Organization for Standardization (ISO)*.

ISO. (2020b). ISO/IEC DIS 27050-4, Information Technology - Electronic Discovery, Part 4: Technical Readiness. *International Organization for Standardization (ISO)*.

ISO. (2022a). ISO/IEC 2005:2022, Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks. *International Organization for Standardization (ISO)*.

ISO. (2022b). ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. *International Organization for Standardization (ISO)*.

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science*. https://doi.org/10.1007/978-3-319-10632-8

Jones, J. (2019, 28/12/22). An Adoption Guide For FAIR - Enabling Cost-Effective Decision Making.

Lalonde, C., & Boiral, O. (2012, 11/01). Managing risks through ISO 31000: A critical analysis. *Risk Management, 14*, 272-300. https://doi.org/10.1057/rm.2012.9

Li, J., & Pang, Z. (2020, 27-29 March 2020). Research on Connotation, Rules and Practice of Adopting International Standards. 2020 6th International Conference on Information Management (ICIM),

Maneerattanasak, U., & Wongpinunwatana, N. (2017, 16-17 July 2017). A proposed framework: An appropriation for principle and practice in information technology risk management. 2017 International Conference on Research and Innovation in Information Systems (ICRIIS),

March, S., & Storey, V. (2008, 12/01). Design science in the information systems discipline: An introduction to the special issue on design science research. *MIS Quarterly, 32*. https://doi.org/10.2307/25148869

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013, 2013/09/01). Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in is Research. *Journal of Computer Information Systems, 54*(1), 11-22. https://doi.org/10.1080/08874417.2013.11645667

Matsuoka, T. (2013, 03/01). A Monte Carlo simulation method for system reliability analysis. *Nuclear Safety and Simulation, 4*, 44-52.

Mayer, N., & Aubert, J. (2020). A risk management framework for security and integrity of networks and services. *Journal of Risk Research*, 1-12. https://doi.org/10.1080/13669877.2020.1779786

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2019, 2019/06/01). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling, 18*(3), 2285-2312. https://doi.org/10.1007/s10270-018-0661-x

McShane, M. (2018). Enterprise risk management: history and a design science proposal. *The Journal of Risk Finance, 19*(2), 137-153. https://doi.org/10.1108/JRF-03-2017-0048

Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A framework for enterprise risk identification and management: the resource-based view. *Managerial Auditing Journal, 34*(2), 162-188. https://doi.org/10.1108/MAJ-12-2017-1751

Nieto, A., Rios, R., & Lopez, J. (2017, 1-4 Aug. 2017). A Methodology for Privacy-Aware IoT-Forensics. 2017 IEEE Trustcom/BigDataSE/ICESS,

NIST. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37 Revision 2. *National Institute of Standards and Technology (NIST)*.

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Revision 5.

Nowell, L., Norris, J., White, D., & Moules, N. (2017, 10/03). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative, 16*. https://doi.org/10.1177/1609406917733847

Nunamaker, J. F., Chen, M., & Purdin, T. D. M. (1990). Systems Development in Information Systems Research. *Journal of Management Information Systems, 7*(3), 89-106. http://www.jstor.org.ezproxy.aut.ac.nz/stable/40397957

O'Reilly, P. (2019, 28/12/2022). The FAIR Model Explained in 90 Seconds. *RiskLens Blog*.

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). *Outline of a design science research process*. https://doi.org/10.1145/1555619.1555629

Ogunsola, A., & Mariscotti, A. (2013). Standards and Standardization. In A. Ogunsola & A. Mariscotti (Eds.), *Electromagnetic Compatibility in Railways: Analysis and Management* (pp. 217-314). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-30281-7_6

Okoli, C., & Nguyen, J. (2015, 01/01). Business Models for Free and Open Source Software. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2568185

Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). *Design Science Research Evaluation* (Vol. 7286). https://doi.org/10.1007/978-3-642-29863-9_29

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007, 2007/12/01). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, 24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Rashid, D. Y., Rashid, A., Warraich, M., Sabir, S., & Waseem, A. (2019, 07/01). Case Study Method: A Step-by-Step Guide for Business Researchers. *International Journal of Qualitative Methods, 18*, 160940691986242. https://doi.org/10.1177/1609406919862424

Rebelo, M. F., Silva, R., Santos, G., & Mendes, P. (2016). Model based integration of management systems (MSs) – case study. *The TQM Journal, 28*(6), 907-932. https://doi.org/10.1108/TQM-09-2014-0079

RiskLens, A. (2020). *FAIR Analysis Fundamentals: Course Workbook*. RiskLens Academy.

SABSA. (2021). *T100 Modelling SABSA with ArchiMate Release 2.0*. SABSA.

Schneider, R. M. (2010). *A comparison of information security risk analysis in the context of e-government to criminological threat assessment techniques* 2010 Information Security Curriculum Development Conference, Kennesaw, Georgia. https://doi.org/10.1145/1940941.1940966

Shamala, P., Ahmad, R., & Yusoff, M. (2013, 2013/07/01/). A conceptual framework of info structure for information security risk assessment (ISRA). *Journal of Information Security and Applications, 18*(1), 45-52. https://doi.org/https://doi.org/10.1016/j.jisa.2013.07.002

Shin, D.-H., Kim, H., & Hwang, J. (2015, 2015/02/01/). Standardization revisited: A critical literature review on standards and innovation. *Computer Standards & Interfaces, 38*, 152-157. https://doi.org/https://doi.org/10.1016/j.csi.2014.09.002

Smith, B. (2020). Announcing Loss Exceedance Charts in the FAIR-U Training App. *FAIR Institue Blog*.

Snyder, H. (2019, 2019/11/01/). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333-339. https://doi.org/https://doi.org/10.1016/j.jbusres.2019.07.039

Suarez, T. (2017, 14/03/2022). A Crash Course on Capturing Loss Magnitude with the FAIR Model. *FAIR Institute Blog*.

Syalim, A., Hori, Y., & Sakurai, K. (2009, 16-19 March 2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. 2009 International Conference on Availability, Reliability and Security,

Torres-Carrión, P. V., González-González, C. S., Aciar, S., & Rodríguez-Morales, G. (2018, 17-20 April 2018). Methodology for systematic literature review applied to engineering and education. 2018 IEEE Global Engineering Education Conference (EDUCON),

von Faber, E. (2014, 2014//). In-House Standardization of Security Measures: Necessity, Benefits and Realworld Obstructions. ISSE 2014 Securing Electronic Business Processes, Wiesbaden.

Vorster, A., & Labuschagne, L. (2005, 07/20). A framework for comparing different information security risk analysis methodologies. *Pages*, 95-103.

Wang, J., Neil, M., & Fenton, N. (2020, 2020/02/01/). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security, 89*, 101659. https://doi.org/https://doi.org/10.1016/j.cose.2019.101659

Wangen, G. (2017). Information Security Risk Assessment: A Method Comparison. *Computer, 50*(4), 52-61. https://doi.org/10.1109/MC.2017.107

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018, 2018/11/01). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security, 17*(6), 681-699. https://doi.org/10.1007/s10207-017-0382-0

Wieringa, R. (2014). *Design Science Methodology for Information Systems and Software Engineering*. https://doi.org/10.1007/978-3-662-43839-8

Appendix A1 – Ethics Exception

Exceptions to activities requiring AUTEC approval (6.7)

The following activities do not require AUTEC approval: *"6.7. Where a professional or expert opinion is sought, except where this is part of a study of the profession or area of expertise".*

Reference:

https://www.aut.ac.nz/research/researchethics/guidelines-and-procedures#6

Appendix A2 – Introduction Letter for Experts Participation

Research Project Motivation Overview

"SECURITY RISK MANAGEMENT FRAMEWORK FOR ISO/IEC 27050 STANDARD"

The gap to fill is RISK management in relation to Electronic Discovery (ED) processes. The ISO/IEC International Standardization for Electronic Discovery has been published in four parts:

- Part 1: The Overview & Concepts
- Part 2: Governance & Management
- Part 3: Code of Practice
- Part 4: Technical Readiness

The challenge for a practitioner is to have a ready reference model to guide information security actions at each process step of the ISO/IEC 27050 ED guidance as illustrated in Figure 1.

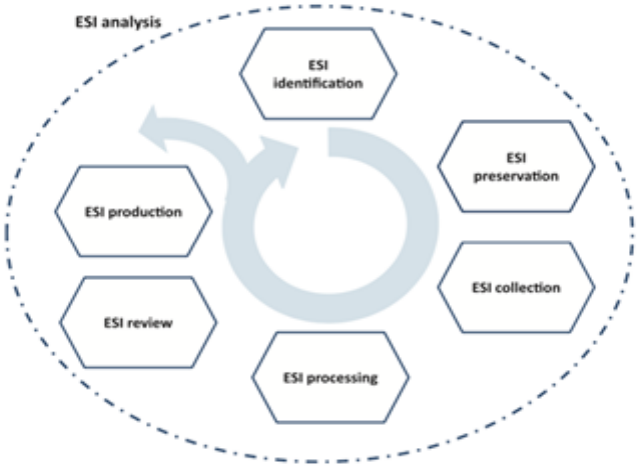


Figure 1: ED process phases (ISO/IEC 27050-1)

This research has analysed the Standard contents and identified security and risk gaps. The deliverable I am sharing with you is my current thinking for a working reference document that Practitioners / Investigators can use to guide and audit their practice and readiness to secure the ED processes.

I invite your feedback to further guide and develop my thinking and to improve the current framework.

Thank you for your help in advance.

Regards,

Nabeel Albahbooh

Figure A2.1: Introductory Letter for Experts Participation

Appendix A3 – Expert Feedback Template

Industry feedback on artefacts is permitted by AUTEC rule 6.7.

Please enter your comments below

Table A3.1: Expert Feedback Template

No.	Questions	Feedback				
	What is your role?					
	How long have you been in the industry?					
1= Excellent 2=Good 3= Ok 4=Poor 5= Change						
	Delete Number of Choice. Put X. Example 2 is chosen. ***Don't Know = leave unmarked.***	**1**	**2**	**3**	**4**	**5**
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	**1**	**2**	**3**	**4**	**5**
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	**1**	**2**	**3**	**4**	**5**
3	How useful is the proposed artefact for your workplace?	**1**	**2**	**3**	**4**	**5**
4	Does the proposed artefact align with the international security risk management standards?	**1**	**2**	**3**	**4**	**5**
5	Is it usable?	**1**	**2**	**3**	**4**	**5**

6	Will it improve risk management?	**1**	**2**	**3**	**4**	**5**
7	Should the artefact be improved?	**1**	**2**	**3**	**4**	**5**
8	Should modifications be made to any component of the proposed artefact?	**1**	**2**	**3**	**4**	**5**
9	List strengths.					
10	List weaknesses and improvements.					
Any Other Comments:						

Appendix A4 – Expert Feedback Records

Expert 1 Feedback

Table A4.1: Expert 1 Feedback

No.	Question	Expert 1 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Good
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Ok
3	How useful is the proposed artefact for your workplace?	Ok
4	Does the proposed artefact align with the international security risk management standards?	
5	Is it usable?	
6	Will it improve risk management?	Ok
7	Should the artefact be improved?	Good
8	Should modifications be made to any component of the proposed artefact?	Ok
9	List strengths.	I reckon it's solid
10	List weaknesses and improvements.	As an improvement would you consider adding a feedback loop from risk treatment back to the risk level. The objective is to re-assess the level after being treated.
	Any Other Comments	

Expert 2 Feedback

Table A4.2: Expert 2 Feedback

No.	Question	Expert 1 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Good
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Good
3	How useful is the proposed artefact for your workplace?	Ok
4	Does the proposed artefact align with the international security risk management standards?	Good
5	Is it usable?	Ok
6	Will it improve risk management?	Ok
7	Should the artefact be improved?	Ok
8	Should modifications be made to any component of the proposed artefact?	Ok
9	List strengths.	Clean and Clear
10	List weaknesses and improvements.	Q5: This depends on the level of understanding of the end user. I understand, as I work with ISO, so it would be useable to me. Q6: For specific use, e-discovery risk as outlined, yes. Q7: Yes:See comments below and attached image. Q8: Yes: See Comments Below.

		Is ‘Vulnerability’ listed in ‘2.Risk Identification’ and ‘3. Risk Estimation’ the same thing? Monitoring and Improvement section: Is there a Metric Determination? Perhaps a ‘Method Selection’ leading to here (which ideally would be designed to produce comparable and reproducible results). As part of my Risk Monitoring process, I look to the objectives to set out what is to be monitored, how it is then measured, who does it, when and how that is sourced and evidenced. Mainly, there are regular internal audits, providing determination of nonconformity / corrective action/improvement"

Expert 3 Feedback

Table A4.3: Expert 3 Feedback

No.	Question	Expert 3 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Ok

2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Poor
3	How useful is the proposed artefact for your workplace?	Ok
4	Does the proposed artefact align with the international security risk management standards?	Ok
5	Is it usable?	Poor
6	Will it improve risk management?	Ok
7	Should the artefact be improved?	Poor
8	Should modifications be made to any component of the proposed artefact?	Ok
9	List strengths.	
10	List weaknesses and improvements.	Every risk has its own situation, therefore it better to focus situation wise risk management framework and better to add risk mitigation components as well.
	Any Other Comments	

Expert 4 Feedback

Table A4.4: Expert 4 Feedback

No.	Question	Expert 4 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Ok
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Ok

3	How useful is the proposed artefact for your workplace?	Poor
4	Does the proposed artefact align with the international security risk management standards?	Good
5	Is it usable?	Poor
6	Will it improve risk management?	Ok
7	Should the artefact be improved?	Poor
8	Should modifications be made to any component of the proposed artefact?	Poor
9	List strengths.	The step looks logical (Phrase name)
10	List weaknesses and improvements.	1. The process over complicated how can we make sure the feasibilities of this process. 2. The framework idea is similar to ISO30001 Risk management. 3. What is your motivation of managing Risk in ISO/IEC 27050-1 4. Can you please provide some risk examples
	Any Other Comments	Not clear about the novelty. The research gap is not clear can you please provide a justification.

Expert 5 Feedback

Table A4.5: Expert 5 Feedback

No.	Question	Expert 5 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Ok
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Good
3	How useful is the proposed artefact for your workplace?	Ok
4	Does the proposed artefact align with the international security risk management standards?	Good
5	Is it usable?	Ok
6	Will it improve risk management?	Ok
7	Should the artefact be improved?	Change
8	Should modifications be made to any component of the proposed artefact?	Change
9	List strengths.	As an initial design, it can be a good start for the research to identify the gap.
10	List weaknesses and improvements.	My comments are in the following section.
	Any Other Comments	"1. As this is an initial design, the information provided are too broad and lacking the proper link. The framework dimensions must be comprehensively around: identify, protect, detect, respond, and recover. What has been stated in the framework, some keywords with incomplete

		processes. Please make sure you align with those dimensions.

Expert 6 Feedback

Table A4.6: Expert 6 Feedback

No.	Question	Expert 5 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Good
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Good
3	How useful is the proposed artefact for your workplace?	Good
4	Does the proposed artefact align with the international security risk management standards?	Excellent
5	Is it usable?	Good
6	Will it improve risk management?	Excellent
7	Should the artefact be improved?	
8	Should modifications be made to any component of the proposed artefact?	
9	List strengths.	All major components are listed. It is seamlessly linked to relevant security standards. Follows the PDCA model
10	List weaknesses and improvements.	Cannot tell unless it is implemented. But since e-Discovery relate to legal aspects, does this comply with the legal and

		regulatory frameworks of the respective countries? That's the reason why gave 2 in some criteria.
	Any Other Comments	

Expert 7 Feedback

Table A4.7: Expert 7 Feedback

No.	Question	Expert 7 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Poor
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Poor
3	How useful is the proposed artefact for your workplace?	Poor
4	Does the proposed artefact align with the international security risk management standards?	Poor
5	Is it usable?	Change
6	Will it improve risk management?	Poor
7	Should the artefact be improved?	
8	Should modifications be made to any component of the proposed artefact?	Ok
9	List strengths.	It attempts to address an issue, as I understood, to identify the uncertainty of the risk assessment part, and proposes an improvement, however, it is not clear at all how this will take place. I see the traditional Risk Analysis, identify inherent risk, evaluate it, and take into consideration the existing controls, relevant

		incident, stakeholders' input, etc. Then attempt to evaluate the Residual risk and recommend further remediation. So, what's new here?
10	List weaknesses and improvements.	1. Lake of clear definition of the issue the proposed framework attempts to solve 2. The diagram requires checking the dataflow to validate the intent of the proposed processes indicated, especially on stage 2 and 3 3. Possibly provide more context to the issue and the proposed solution/improvement
	Any Other Comments	While I mark it a bit low on the scale, I think it needs quite a bit of clarification, improve the diagram workflow, and provide more info on the context.

Expert 8 Feedback

Table A4.8: Expert 8 Feedback

No.	Question	Expert 8 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Good
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Poor
3	How useful is the proposed artefact for your workplace?	Good
4	Does the proposed artefact align with the international security risk management standards?	Ok
5	Is it usable?	Excellent
6	Will it improve risk management?	Good
7	Should the artefact be improved?	Ok
8	Should modifications be made to any component of the proposed artefact?	Ok
9	List strengths.	Any visual representation of what our complex process steps, cleanly and simply laid out, are of value. Therefore, I see the strength of the model is it provides a single point of reference, as a way into what are otherwise dense textual standards.
10	List weaknesses and improvements.	See above, usability, usability, usability. Warren Buffett used to test all his investment concepts with his two maiden aunts to ensure they were communicable and comprehensible. As a standalone artefact, and in the absence of

		the researcher introducing them, the researcher needs to ask himself could someone rapidly understand the way into the model. Hence my view that further focus is required around the introduction as well as Figure 1.
	Any Other Comments	Any Other Comments: I really like the model. From what I see, regardless of the standard being implemented e.g., NIST, ISO, or even in SOC2 type attestations, it can bring structure to the process stages. However, there is no clear one-to-one relationship between Figure 1 and the model per se. What would assist usability is perhaps if there was an alignment with the labels across both diagrams including the 1 through 5 process steps. Perhaps providing a lighter colour coding per step that ties back to Figure 1 would assist. I would suggest lighter shading, as when printed the dark green colouring of the model makes the inbox legends difficult to read.

		Also, in the first sentence immediately below The Figure 1 legend it reads that the research has analyse the standards contents and identified security and risk apps. Should this read, process gaps? A further style point should Nabeel be doing further research rounds maybe his Likert Scale should read -strongly agree through strongly disagree - rather than its current scoring. After all he is measuring the participants level of agreement regarding the relevance of the model. Q2: Note above, I think the model is very good. I've scored this point lowly as it needs more context to draw the reader in necessary to illustrate this usability, and therefore utility. So, this comment does not refer to the strength of the model, rather that it needs a gentler introduction. Q4: See above usability. Which standards?

		Q7: See above. Perhaps, this should be a comments field in future versions of the questionnaire rather than a scale. Q8: See above. Perhaps, this should be a comments field in future versions of the questionnaire rather than a scale.

Expert 9 Feedback

Table A4.9: Expert 9 Feedback

No.	Question	Expert 9 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Good
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Excellent
3	How useful is the proposed artefact for your workplace?	Good
4	Does the proposed artefact align with the international security risk management standards?	Excellent
5	Is it usable?	Good
6	Will it improve risk management?	Ok
7	Should the artefact be improved?	
8	Should modifications be made to any component of the proposed artefact?	
9	List strengths.	Adding data mapping in risk identification is a great option.
10	List weaknesses and improvements.	1. Risk Analysis method under Risk

		Identification in the workflow diagram does not lead to a next step and method is not identified. 2. Options provided to answer most questions does not fit the right answer. For instance, you can't answer the question "Should the artefact be improved?" with excellent.
	Any Other Comments	Q7) Answer does not apply Q8) Question can't be answered with provided options

Expert 10 Feedback

Table A4.10: Expert 10 Feedback

No.	Question	Expert 10 Feedback
1	Overall, how effective do you think the proposed artefact would be for electronic discovery risk management?	Poor
2	Are the defined components of the proposed artefact clear and relevant to what you observe?	Ok
3	How useful is the proposed artefact for your workplace?	Ok

No.	Question	Expert 10 Feedback
4	Does the proposed artefact align with the international security risk management standards?	Poor
5	Is it usable?	OK
6	Will it improve risk management?	Poor
7	Should the artefact be improved?	Poor
8	Should modifications be made to any component of the proposed artefact?	Ok
9	List strengths.	A framework considers why, when, how, and what to assess. It comprised 4 main steps alongside with principles and monitoring. The framework considers the expanding digital footprint of modern organisations which is introducing new security risks. It is look beyond traditional approaches to security risk assessment, detection, and response to manage a wider set of risks. Which helps strategic cybersecurity leaders to demonstrate clear value in the organization's cybersecurity investments.
10	List weaknesses and improvements.	The main issue with this framework is that it needs to be implemented and makes the framework tangible. The framework needs at least two examples and provides evidence of its utility via a naturalistic, summative evaluation through its use on an actual project.
	Any Other Comments	

Appendix B1 – ISO/IEC 31000:2018 Risk Context

ISO/IEC 31000 Principles

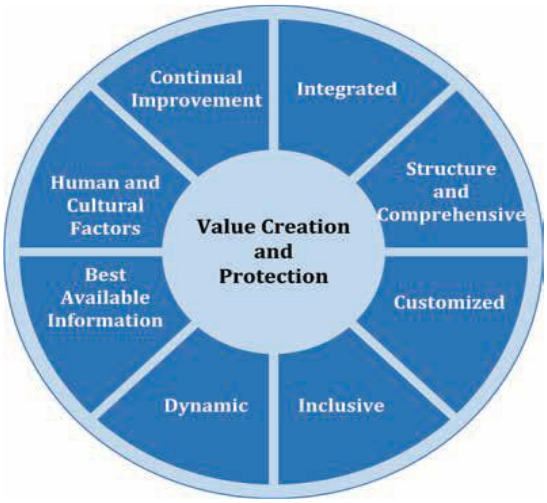


Figure B1.1: ISO/IEC 31000 Principles (ISO, 2018c, p. 3)

ISO/IEC 31000 Framework

Figure B1.2: ISO/IEC 31000 Framework (ISO, 2018c, p. 4)

ISO/IEC 31000 Process

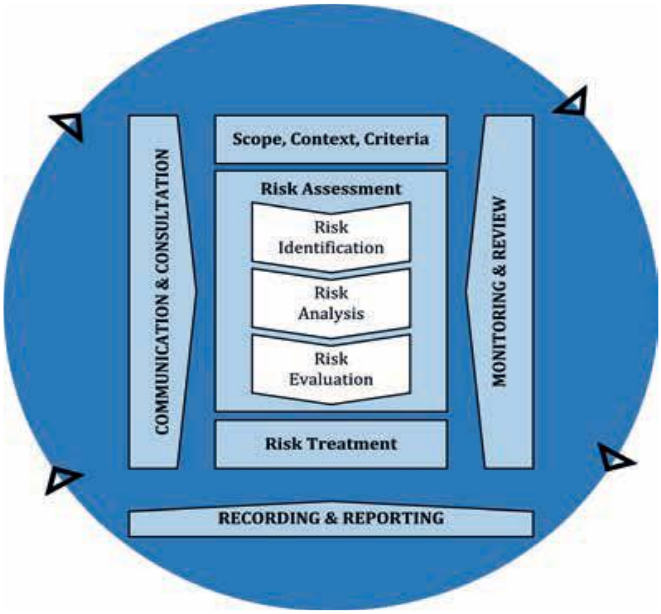


Figure B1.3: ISO/IEC 31000 Process (ISO, 2018c, p. 9)

The ISO/IEC 31000 Principles

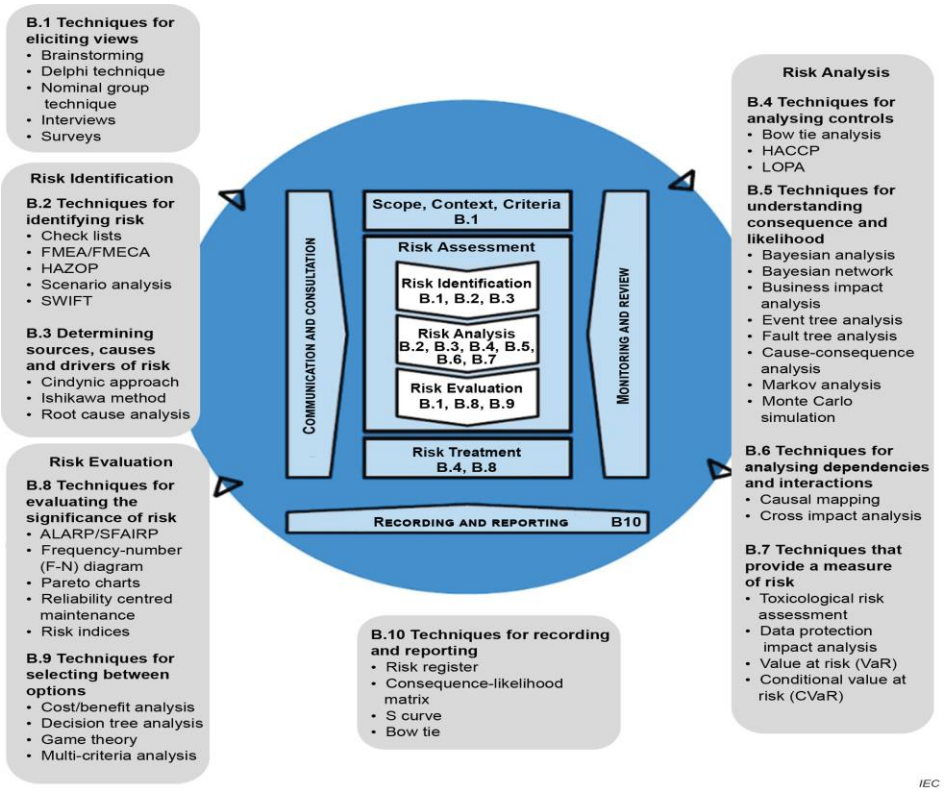


Figure B1.4: Application of Techniques in the ISO/IEC 31000 Process (ISO, 2019, p. 37)

Appendix B2 – ISO/IEC 27005: 2022 Risk Context

ISO/IEC 27005 Process

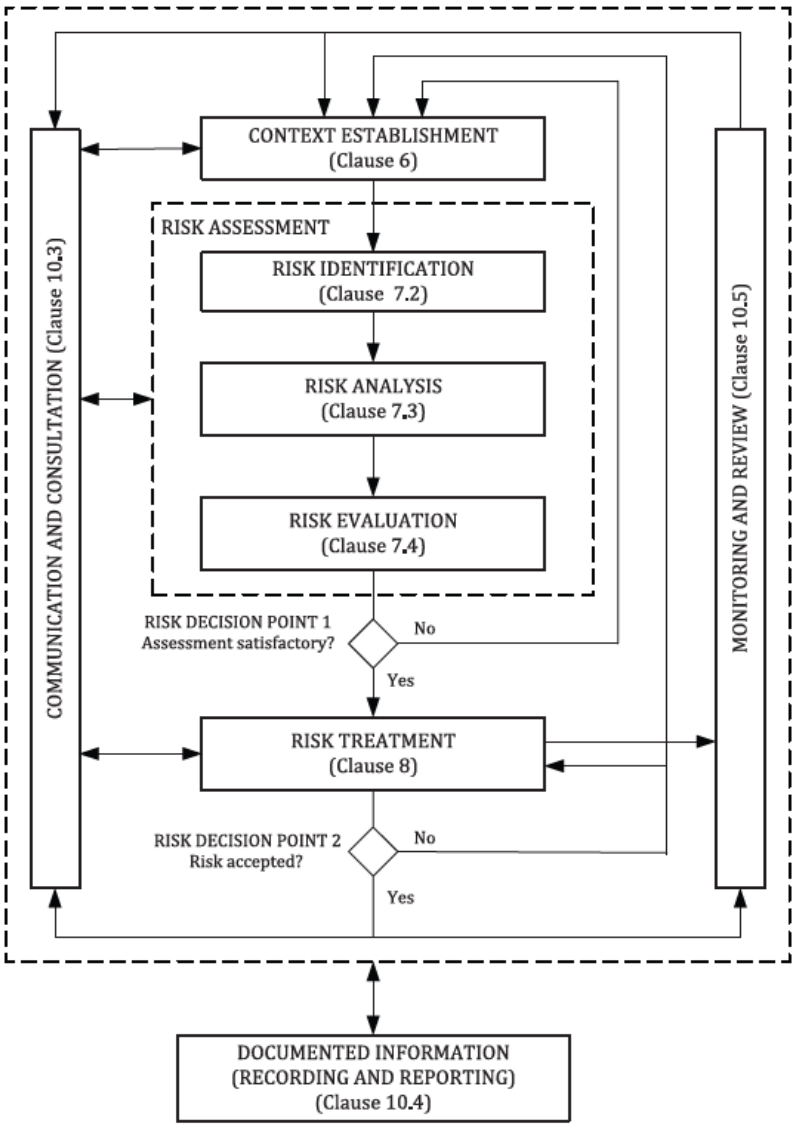


Figure B2.1: Illustration of Risk Management Process in the ISO/IEC 27005 (ISO, 2022a, p. 8)

Risk Appetite Options

Table B2.1: Risk Appetite Options

Option	Description
Treat	An organisation implements a policy to mitigate the risk.
Accept	An organisation may choose to accept the risk because the likelihood of the risk occurring is so minor compared to the cost of treatment (e.g., an earthquake occurring in a geographic area where earthquakes are not common).

Avoid	An organisation may choose to avoid a risk that is deemed unacceptable, and the cost of treatment would outweigh the benefit (e.g., a legacy system that poses specific risks. An organisation may choose to take out the legacy system and therefore, those risks no longer exist).
Transfer	An organisation transfers the risk by purchasing an insurance policy to reduce the impact of the risk.

ISO/IEC 27001 Recommended Controls

Table B2.2: Recommended Security Controls in ISO/IEC 27001: 2022 Standard (ISO, 2022b)

No.	ID	Family
1	A.5	Organisational Controls
2	A.6	People Controls
3	A.7	Physical Controls
4	A.8	Technological Controls

Appendix B3 – NIST 800-53 Risk Context

NIST 800-53 Process

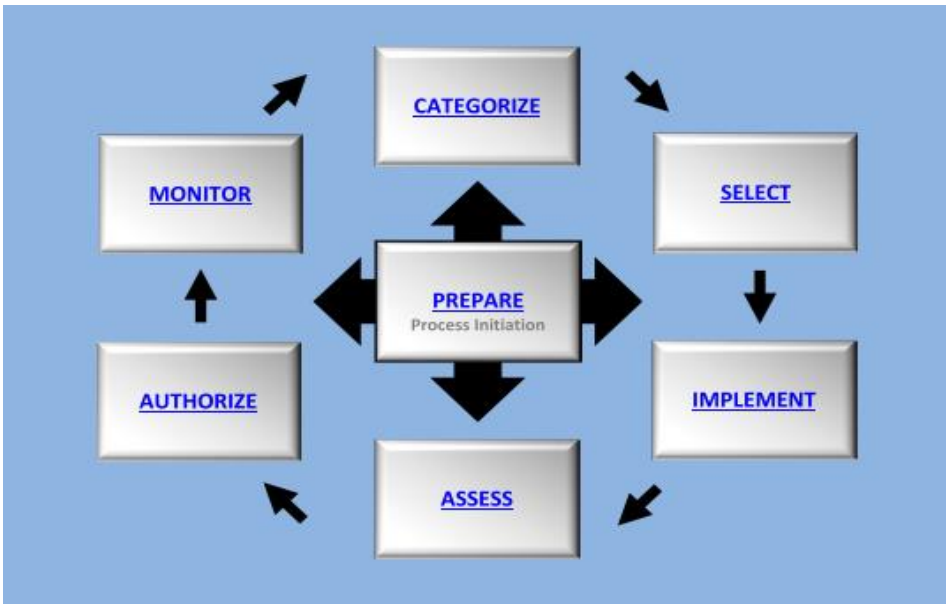


Figure B3.1: Illustration of Risk Management Process in NIST (NIST, 2018, p. 9)

NIST 800-53 Recommended Controls

Table B3.1: Recommended Security and Privacy Controls in NIST 800-53 (NIST, 2020)

No.	ID	Family
1	AC	Access Control
2	AT	Awareness and Training
3	AU	Audit and Accountability
4	CA	Assessment, Authorisation and Monitoring
5	CM	Configuration Management
6	CP	Contingency Planning
7	IA	Identification and Authorisation
8	IR	Incident Response
9	MA	Maintenance
10	MP	Media Protection
11	PE	Physical and Environmental Protection
12	PL	Planning
13	PM	Program Management
14	PS	Personal Security
15	PT	PII Processing and Transparency

No.	ID	Family
16	RA	Risk Assessment
17	SA	System and Services Acquisition
18	SC	System and Communications Protection
19	SI	System and Information Integrity
20	SR	Supply Chain Risk Management

NIST 800-53 Control Structure Example

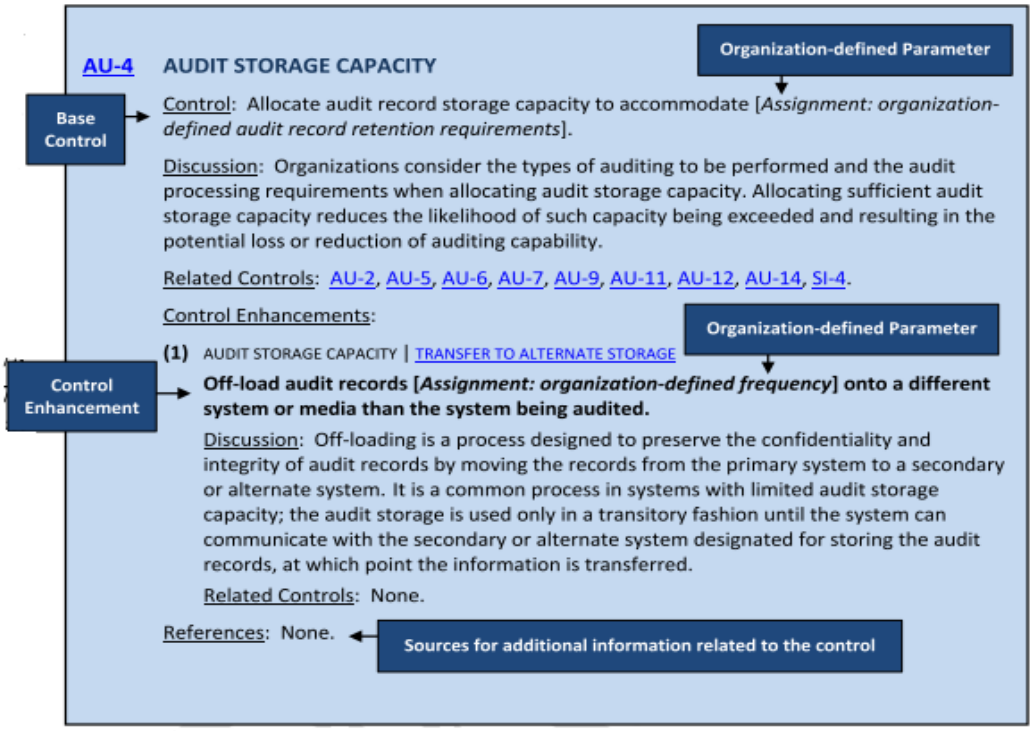


Figure B3.2: Control Structure Example in NIST 800-53 (NIST, 2020, p. 9)

Appendix B4 – ENISA Risk Context

ENISA Risk Management Framework Process

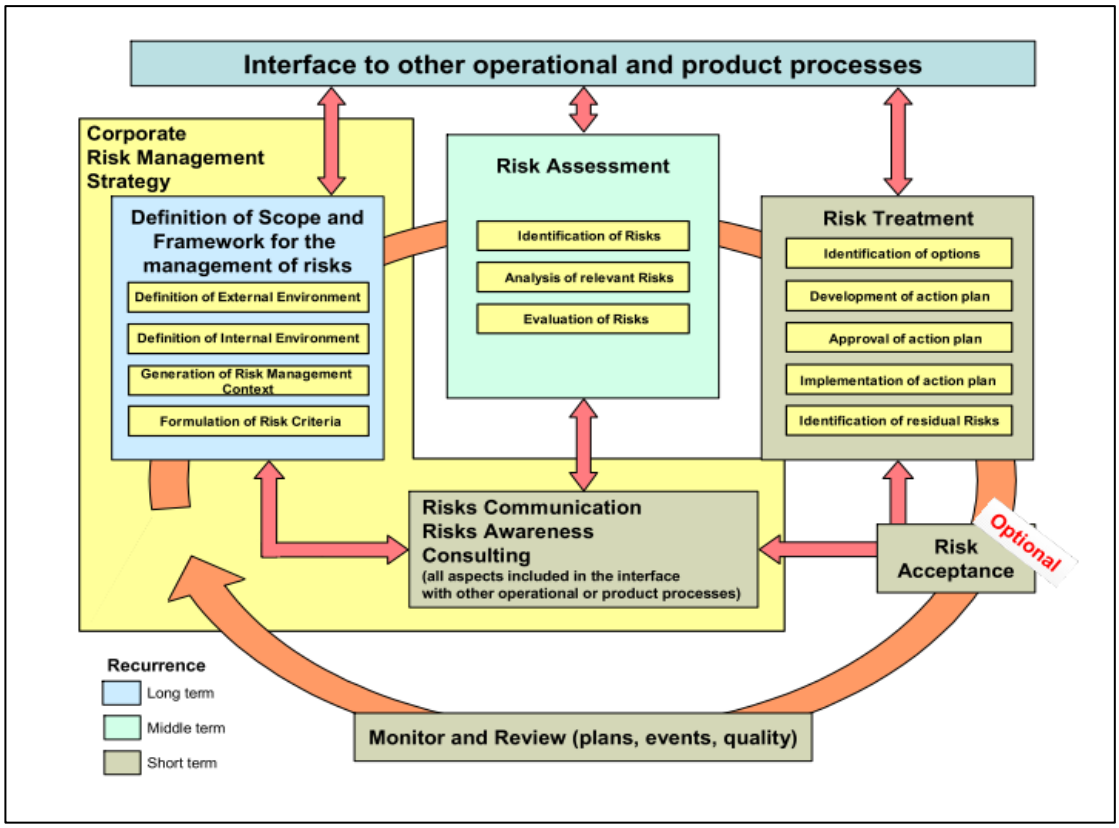


Figure B4.1: Overall Cycle of ENISA Risk Management Framework Process (ENISA, 2006, p. 13)

ENISA Recommended Controls

Table B4.1: Recommended Security Controls in ENISA (ENISA, 2007)

Category	ID	Family
Organisational Controls	SP1	Security Awareness and Training
	SP2	Security Strategy
	SP3	Security Management
	SP4	Security Policies and Regulations
	SP5	Collaborative Security Management
	SP6	Contingency Planning / Disaster Recovery
Asset-Based Controls	OP1	Physical Security
	OP2	Information Technology Security
	OP3	Staff Security

Appendix B5 – The Risk IT Risk Context

The Risk IT Principles

Figure B5.1: The Risk IT Principles (ISACA, 2009a, p. 13)

The Risk IT Framework Process

Figure B5.2: The Risk IT Framework Process (ISACA, 2009a, p. 15)

The Risk IT Controls Set

Table B5.1: The Risk IT Controls Set (ISACA, 2009b)

No.	ID	Control Family
1	Governance	• IT Architecture Board • Definition and Maintenance of Business Functional and Technical Requirements • Risk Analysis Report • Enterprise Information Architecture Model • Relationships
2	Application Software Implementation, Integrity, and Performance	• Major Upgrades to Existing Systems • Application Software Maintenance • Processing Integrity and Validity • Accuracy, Completeness, and Authenticity Checks • Transaction Authentication and Integrity • Development of Application Software • Post-implementation Review • Identity Management • Development and Acquisition Standards • Source Data Preparation and Authorisation
3	Regulatory and Contractual Compliance	• Identification of External Legal, Regulatory, and Contractual Compliance Requirements • Evaluation of Compliance with External Requirements
4	Performance of Third-Party Suppliers	• Supplier Relationship Management • Supplier Risk Management • Supplier Performance Monitoring
5	Staff Security and Skills	• Job Change and Termination • Personnel Training • Job Change and Termination • Personnel Clearance Procedures
6	Infrastructure	• Infrastructure Resource Protection and Availability • Configuration Integrity Review • IT Policies Management • Infrastructure Maintenance • Preventive Maintenance for Hardware • Protection of Security Technology • Change Standards and Procedures • IT Policy and Control Environment

No.	ID	Control Family
7	Physical and Environmental	• Physical Facilities Management • Protection Against Environmental Factors • Physical Security Measures
8	System Capacity	• Performance and Capacity Planning • Current Performance and Capacity • Future Performance and Capacity • IT Resources Availability • Monitoring and Reporting
9	Malware and Logical Attacks	• Security Testing, Surveillance and Monitoring • Malicious Software Prevention, Detection, and Correction • Network Security • Application Security and Availability • Management of IT Security • User Account Management • Exchange of Sensitive Data
10	Information Media	• Storage and Retention Arrangements • Disposal • Backup and Restoration • Exchange of Sensitive Data • Sensitive Documents and Output Devices
11	Data Integrity	• Data Classification Scheme • Impact Assessment, Prioritisation, and Authorisation • Security Requirements for Data Management
12	Recovery	• IT Services Recovery and Resumption • IT Continuity Plans

Appendix B6 – ISO/IEC 27050 Risk Context

ISO/IEC 27050 Series

Table B6.1: ISO/IEC 27050 Standard Series Description (ISO, 2018a, 2018b, 2020a, 2020b)

ISO Standard Name	Description	Challenges Addressed
Part 1 – ISO/IEC 27050-1:2019 (Overview and Concepts)	It provides a general understanding of eDiscovery terminology, concepts and objectives, types, sources, and representations. It also describes the ESI governance and readiness as well as the eDiscovery phases from a high-level perspective.	Setting a collective understanding of various concepts and terminology for eDiscovery.
Part 2 – ISO/IEC 27050-2:2018 (Guidance for Governance and Management of Electronic Discovery)	It provides details about the governance and management aspects of eDiscovery. It also describes how eDiscovery is aligned with the governance principles from an organisation perspective.	Providing a practical and cost-effective way for personnel involved in managing eDiscovery activities. Promoting consideration of using a proactive technology to minimise costs and risks, while increasing efficiencies throughout the eDiscovery process.
Part 3 – ISO/IEC 27050-3:2020 (Code of Practice for Electronic Discovery)	It addresses various aspects of each eDiscovery phase (i.e., overview, objectives, considerations, requirements, and guidance). It also provides further materials that can help practitioners understand the eDiscovery phases activities in more depth.	Identifying the required competency for personnel involved in the eDiscovery. Recommending effective ways to avoid disclosures of ESI.
Part 4 – ISO/IEC 27050-4:2020 (Technical Readiness)	It guides how an organisation can plan, prepare, and implement the eDiscovery phases from knowledge, skills, processes, and technologies perspectives. It also includes a questionnaire (Annex A) with a list of questions that can help an	Communicating objectives and risks are inherent in the eDiscovery process.

	organisation with the ESI storage investigation.	

Governance of Digital Forensic Risk Framework

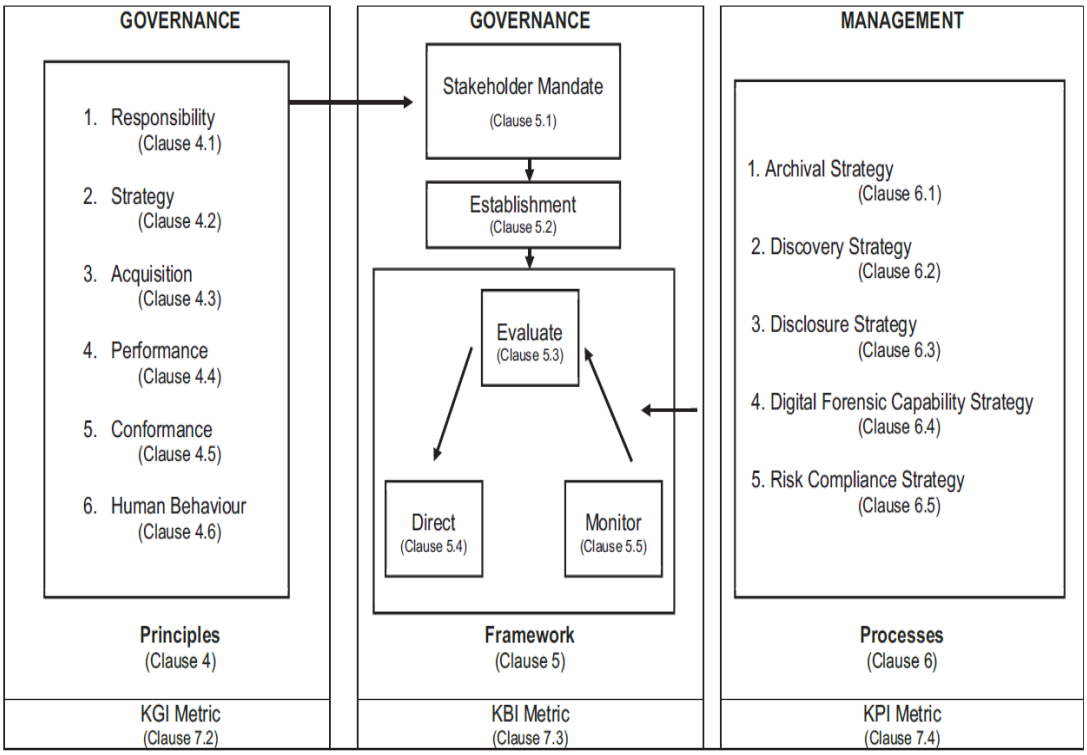


Figure B6.1: Governance of Digital Forensic Risk Framework (ISO, 2016, p. 5)

Electronic Discovery Phases and Relationship with Data Analytics

Table B6.2: Electronic Discovery Phases and Relationship with Data Analytics

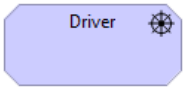
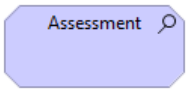
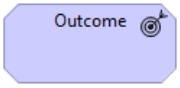
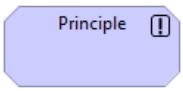
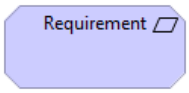
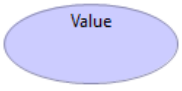
Phase	Data Analytics Supporting
Identification	Finding ESI sources holding information potentially relevant to the requested production.
Preservation	Developing an ESI preservation plan that is proper and executed appropriately.
Collection	Ensuring that the collection team has the required information and has met its goals.
Processing	Preparing the collected data for ESI review to confirm the results.
Review	Confirming ESI review has met its goals effectively and efficiently.
Production	Delivering ESI to the recipient of production in an agreed and consistent format.

Appendix C1 – ArchiMate 3.1 Elements

ArchiMate 3.1 Motivation Elements

Motivation elements form an independent aspect that models the intent and purpose of the architectural design and can be placed in any layer. The set of Motivation elements used in the Artefact 2 is shown in Table C.1 with a description.

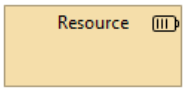
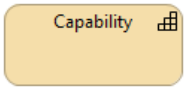
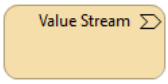
Table C1.1: ArchiMate 3.1 Motivation Elements

Element / Notation	Definition
	The role of an individual, team, or organisation that represents their interests in the outcome of the architecture.
	An external or internal condition motivates an organisation to define its goals and implement the changes necessary to achieve them.
	A gap analysis comparing the current state of some stakeholder concern(s) and a future desired state.
	A high-level statement of intent, direction, or desired end state for an organisation and its stakeholders.
	A result that has been achieved.
	A Principle represents a statement of intent defining a general property that applies to any system in a certain context in the architecture.
	A statement of need that must be met by the architecture.
	The relative worth, utility, or importance of a core element or an outcome.

ArchiMate 3.1 Strategy Elements

The Strategy elements are used to model business strategy and capability-based planning. The notations used in Artefact 2 are shown in Table C.2.

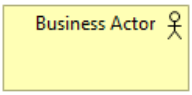
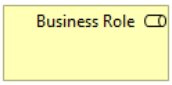
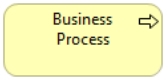
Table C1.2: ArchiMate 3.1 Strategy Elements

Element / Notation	Definition
	An asset owned or controlled by an individual or organisation.
	An ability that an active structure element, such as an organisation, person or system, possesses.
	A value stream represents a sequence of activities that create an overall result for a customer, stakeholder, or end-user.

ArchiMate 3.1 Business Elements

ArchiMate 3.1 provides type definitions for actors, processes, and data, but not individual persons, process executions, or documents. The definition and notation for Business elements used in the Artefact 2 are shown in Table C.3.

Table C1.3: ArchiMate 3.1 Business Elements

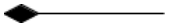
Element / Notation	Definition
	A business entity that can perform a behaviour.
	The responsibility for performing specific behaviour, to which an actor can be assigned, or the part an actor plays in a particular action or event.
	A sequence of business behaviours that achieves a specific outcome, such as a defined set of products or business services.

ArchiMate 3.1 Relationship Notations

Relationships are directional and connect exactly two endpoints, but they can be extended by using 'junction connectors' that allow, for example, the splitting and joining of data flows. The definition and notation for each of these relationships are shown in Table C.4.

Table C1.4: ArchiMate 3.1 Relationships

Relationship	Definition	Notation
Structural Relationships		

Relationship	Definition	Notation
Composition	Indicates that an element consists of one or more other elements.	
Assignment	Expresses the allocation of responsibility, the performance of behaviour, and execution.	
Dependency Relationships		
Serving	Models that an element provides its functionality to another element.	
Influence	Models that an element affects the implementation or achievement of some motivation element, either positively or negatively.	
Dynamic Relationships		
Trigrining	Describes a temporal or causal relationship between elements.	
Flow	Describes a temporal or causal relationship between elements.	
Connection Relationships		
Junction	connects relationships of the same type (e.g., And-Junction).	

Appendix D1 – FAIR Model

Forms of Loss Subcomponents

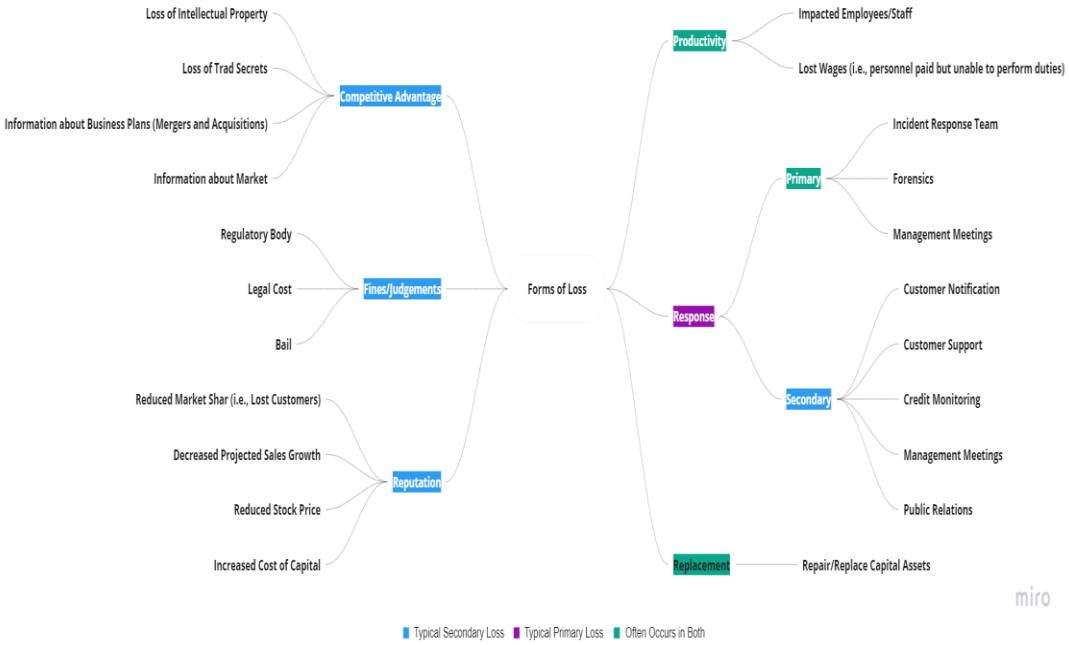


Figure D1.1: Forms of Loss Subcomponents derived from (Suarez, 2017)

FAIR Model Formulas

Table D1.1: Output and Input Factors and Function Used in the Proposed Risk Management Model

EQU#	Output Factor	Input Factor	Function
1	Annualized Loss Exposure (Risk Level): R_{ALE}	Impact: I Likelihood: L	$R_{ALE} = I \times L$
2	Likelihood: L	Threat Probability: T_{PRB} Vulnerability: V	$L = T_{PRB} \times V$
3	Impact: I	Primary Loss: L_P Secondary Loss: L_S	$I = L_P + L_S$
4	Primary Loss: L_P	Primary Productivity Loss: L_{PPRO} Primary Response Loss: L_{PRES} Primary Replacement Loss: L_{PREP}	$L_P = L_{PPRO} + L_{PRES} + L_{PREP}$
5	Primary Productivity Loss: L_{PPRO}	Number of Employees/Staff Impacted: E_{PPRO} Employee/Staff Hourly Rate: R_{PPRO}	$L_{PPRO} = E_{PPRO} \times R_{PPRO}$
6	Primary Response Loss: L_{PRES}	Number of Employees/Staff Involved in Incident Response: E_{PRES} Incident Response Team Hourly Rate (Internal): H_{PRES} **Incident Response Cost: C_{PINC}** **Foriensic Response Team Cost (External): C_{PFOR}** Number of Hours Spent during Meeting: H_{PMET}	$L_{PRES} = C_{PINC} + C_{PFOR} + C_{PMGT} = (E_{PRES} \times H_{PRES}) + C_{PFOR} + (H_{PMET} \times C_{PAVG})$

		Average Cost per Meeting: C_{PAVG} **Management Meetings Cost: C_{PMGT}**	
7	Primary Replacement Loss: L_{PREP}	Replacement Cost: C_{PREP}	$L_{PREP} = C_{PREP}$
8	Secondary Loss: L_S	Secondary Response Loss: L_{SRES} Secondary Competitive Advantage Loss: L_{SCOM} Secondary Fines / Judgements Loss: L_{SFIN} Secondary Reputation Loss: L_{SREU}	$L_S = L_{SRES} + L_{SCOM} + L_{SFIN} + L_{SREU}$
9	Secondary Response Loss: L_{SRES}	Cost per Customer: C_{SCUS} Number of Compromised Accounts/Records/Cases: N_{SCOM} **Customer Notification Cost: C_{SNOT}** Number of Affected Customers: N_{SAFF} Average Customer Support Cost per Customer: C_{SAVG} **Customer Support Cost: C_{SUP}** Avarge Cost per Monitoring: C_{SAVG1} **Credit Monitoring: C_{SMON}** Number of Hours Spent during Meeting: H_{SMET} Average Cost per Meeting: C_{SAVG2} **Management Meetings Cost: C_{SMGT}** Random Percentage for Public: P_{PRAN1} **Public Relations Cost: C_{SPUB}**	$L_{SRES} = C_{SNOT} + C_{SUP} + C_{SMON} + C_{SMGT} + C_{SPUB}$ $= (C_{SCUS} \times N_{SCOM}) + (N_{SAFF} \times C_{SAVG} \times C_{SCOM}) + (N_{SAFF} \times C_{SAVG1} \times C_{SCOM}) + (H_{SMET} \times C_{SAVG2}) + (C_{SCOM} \times P_{PRAN1})$

10	Secondary Competitive Advantage Loss: L_{SCOM}	Competitive Advantage Cost: C_{SCOM}	$L_{SCOM} = C_{SCOM}$
11	Secondary Fines / Judgements Loss: L_{SFIN}	Number of Compromised Accounts/Records/Cases: N_{SCOM} Random Percentage for Legal: P_{PRAN2} **Legal Cost: C_{SLEG}**	$L_{SFIN} = N_{SCOM} \times P_{PRAN2}$
12	Secondary Reputation Loss: L_{SREU}	Number of Compromised Accounts/Records/Cases: N_{SCOM} Average Profile per Customer Cost: C_{SPOF}	$L_{SREU} = N_{SCOM} \times C_{SPOF}$
13	Threat Probability: T_{PRB}	Number of Possible Incidents per Year (a threat agent will act against an asset): NINC Threat Probability Qualitative Scale: T_{SCL1} For example: • Very High (VH) = 50 times per year • High (H) = Between 20 and 50 times per year • Moderate (M) = Between 1 and 20 times per year • Low (L) = Between 0.1 and 2 times per year • Very Low (VL) = <0.1 times per year (less than once every 20 years)	$T_{PRB} = T_{SCL1} = LUT (N_{INC})$
14	Vulnerability: V	Threat Capability: T_{CAP} Control Strength: C_{STR}	$V = MC (T_{CAP}, C_{STR})$

15	Threat Capability: T_{CAP}	Percentile of a Threat Agent Capabilities: P_{AGE} Threat Capability Qualitative Scale: T_{SCL2} For example: • Very High (VH) = Top 2% when compared against the overall threat population (98th percentile) • High (H) = Top 16% when compared against the overall threat population (between the 84th and 98th percentiles) • Moderate (M) = Average skill and resources, between the bottom 16% and top 16% (between the 16th and 84th percentiles) • Low (L) = Bottom 16% when compared against the overall threat population (below the 16th percentile) • Very Low (VL) = Bottom 2% when compared against the overall threat population (below the 2nd percentile)	$T_{CAP} = T_{SCL2} = LUT (P_{AGE})$
16	Control Strength: C_{STR}	Percentile of a Control Effectiveness: P_{CON} Control Strength Qualitative Scale: T_{SCL3} For example: • Very High (VH) = Protects against all but the top 2% of an average threat population (98th percentile) • High (H) = Protects against all but the top 16% of an average threat population (between the 84th and 98th percentiles) • Moderate (M) = Protects against the average threat agent (between the 16th and 84th percentiles)	$C_{STR} = T_{SCL3} = LUT (P_{CON})$

		• Low (L) = Only protects against the bottom 16% of an average threat population (below the 16th percentile) • Very Low (VL) = Only protects against the bottom 2% of an average threat population (below the 2nd percentile)	