A MODEL-DRIVEN FRAMEWORK TO SUPPORT ANALYSIS AND IMPLEMENTATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS

DANIEL GANJI

A thesis submitted in partial fulfilment of the
requirements of the University of Brighton
for the degree of Doctor of Philosophy

December 2019

Abstract

Information is fast becoming a vital instrument in business operations, with the last two decades have seen a growing trend in information security breaches. The principles of ISO/IEC 27001 Standard provide a significant area of interest for organisations to preserve the confidentiality, integrity, and availability of information. The standard is a set of interlinked requirements under one process known as Information Security Management Systems (ISMS). It has been an increasing interest in conforming with the standard from a wide range of industries in the past decade. Along with this growth in the standard, however, organisations have accentuated an increasing concern on understanding the requirements of the standard.

This thesis observed a decline in methods to enable implementation of ISMS despite the high interest from industries. Results from the investigation of the literature conclusively reported, that the existing research has been restricted to limited aspects of the standard and most of the studies suffered from lack of a robust theoretical framework to address all or most parts of the ISMS. This thesis adopts a methodological approach found by evaluating the current gap in the literature, explores the underlying needs of organisations, and an in-depth analysis of the standard. A novel technique utilised, integrating concepts from the security requirements engineering and specifications of the standard to propose INtegratable Framework for mOdelling Requirements of Management Systems (INFORMS).

A model-driven framework for organisations to gain further understanding of the standard and to support analysis and implementation of information security management systems. This thesis uses security-oriented goal models to coherently capture the multi-faceted structure of organisations, steered by a set of explicit rules from the standard. The key outcome of this research contributes towards two main directions of a modelling language and a framework, an original approach to model the requirements of the standard. The evaluation of INFORMS indicated that the developed framework provides a holistic approach to information security practitioners, developers, and top management to protect information assets.

Contents

List of Tables viii

List of Figures xi

Acronyms xii

1 Introduction 1

1.1 Motivation . . . 2
1.2 Research Questions . . . 4
1.3 Aim and Objectives . . . 4
1.4 Thesis Structure . . . 4

2 Literature Review 6

2.1 Background . . . 6
2.1.1 Requirements Engineering . . . 6
2.1.2 Information Security Frameworks . . . 10
2.2 Investigation of Related Work . . . 21
2.2.1 Review Protocol . . . 21
2.2.2 Results . . . 26
2.2.3 Discussion . . . 32
2.3 Research Gaps and Challenges . . . 37
2.4 Research Baseline . . . 38
2.4.1 Goal-Oriented Requirements Engineering . . . 38
2.4.2 Diagramming Platforms . . . 39
2.5 Summary . . . 40

3 INFORMS Modelling Language 42

3.1 Requirements of the Modelling Language . . . 42
3.2 Modelling Language Overview . . . 43
3.3 Concepts . . . 46
3.3.1 Actor . . . 46

3.3.2 Asset . . . 47
3.3.3 Constraint . . . 49
3.3.4 Goal . . . 50
3.3.5 Objective . . . 51
3.3.6 Role . . . 52
3.3.7 Task . . . 54
3.3.8 Threat . . . 56
3.3.9 Treatment . . . 57
3.3.10 Vulnerability . . . 58
3.4 Relationships . . . 59
3.4.1 Conduct . . . 59
3.4.2 Define . . . 60
3.4.3 Dependency . . . 60
3.4.4 Exploit . . . 61
3.4.5 Harm . . . 61
3.4.6 Impact . . . 62
3.4.7 Include . . . 63
3.4.8 Mitigate . . . 64
3.4.9 Restrict . . . 64
3.4.10 Satisfy . . . 64
3.5 Summary . . . 65

4 INFORMS Framework 66
4.1 Framework Overview . . . 66
4.1.1 Framework Workflow . . . 70
4.1.2 Presentation . . . 72
4.1.3 General Structure of Views . . . 74
4.2 Strategic Viewpoint . . . 77
4.2.1 Scope . . . 77
4.2.2 Leadership . . . 78
4.2.3 Policy . . . 79
4.2.4 Awareness . . . 80
4.2.5 Communication . . . 82
4.2.6 Documented Information . . . 83
4.3 Operational Viewpoint . . . 85
4.3.1 Actors Description . . . 86
4.3.2 Constraints Specification . . . 88
4.3.3 Asset Management . . . 89

4.3.4 Goal Delivery . . . 91
4.4 Technical Viewpoint . . . 92
4.4.1 Identification of Threats . . . 94
4.4.2 Identification of Vulnerabilities . . . 97
4.4.3 Assessment of Impacts . . . 99
4.4.4 Risk Determination . . . 104
4.4.5 Risk Evaluation . . . 106
4.4.6 Risk Treatment . . . 108
4.4.7 Risk Acceptance . . . 111
4.5 System Viewpoint . . . 112
4.5.1 Roles Description . . . 112
4.5.2 Objectives Specification . . . 113
4.6 Standard Viewpoint . . . 116
4.6.1 Monitoring and Measurement . . . 116
4.6.2 Internal Audit . . . 118
4.6.3 Management Review . . . 120
4.6.4 Nonconformities and Corrective Action . . . 121
4.6.5 Continual Improvement . . . 122
4.7 Summary . . . 124

5 Evaluation **125**
5.1 Evaluation Method . . . 125
5.1.1 Case Study . . . 126
5.2 Case Study Design and Planning . . . 127
5.2.1 Objectives . . . 128
5.2.2 Units of Analysis . . . 128
5.2.3 Methods of Data Collection . . . 128
5.2.4 Selection of Data . . . 129
5.2.5 Case Selection Strategy . . . 130
5.2.6 Ethical Considerations . . . 130
5.2.7 Data Collection . . . 130
5.3 Application of Framework . . . 134
5.3.1 Strategic Viewpoint . . . 135
5.3.2 Operational Viewpoint . . . 138
5.3.3 Technical Viewpoint . . . 149
5.3.4 System Viewpoint . . . 165
5.3.5 Standard Viewpoint . . . 169
5.4 Evaluation Results . . . 175

5.4.1 Metrics Evaluation 176
5.4.2 Stakeholders Interview 179
5.5 Summary 182

6 Conclusion **183**
6.1 Revisiting the Aim and Objectives 183
6.2 Main Contributions 185
6.3 Future Directions 187
6.4 Summary 189

Glossary **190**

Bibliography **193**

Appendix A Threat Catalogue **208**

Appendix B Vulnerability Catalogue **211**

Appendix C Statement of Applicability **214**

Appendix D Publication **216**

List of Tables

2.1 Top-to-bottom approach to IS standards and frameworks 13
2.2 ISO/IEC 27000 family of standards 19
2.3 PRESS checklist 23
2.4 Overall description of primary studies 33
2.5 Detailed view of the primary studies 35
2.6 Diagramming platform comparison 40

4.1 Methods in presenting views 74
4.2 Documented information assignment 84
4.3 Likelihood level definitions 97
4.4 Ease of exploit level definitions 98
4.5 Level definitions of the impacts on elements of asset 100
4.6 Level definitions of the impacts on elements of goal 102
4.7 Impact matrix 104
4.8 Evaluation criteria for Asset Risk Indicator 107
4.9 Evaluation criteria for Goal Risk Indicator 108
4.10 Views with assigned responsibility 114

5.1 Gap analysis of the AHC's documents and records 133
5.2 Annual awareness and education programme - AHC 137
5.3 Documented information checklist - AHC 138
5.4 Description of the actors - AHC 139
5.5 Specification of the constraints - AHC 141
5.6 Inventory of assets - AHC 142
5.7 Goals and dependencies - AHC 144
5.8 Threats and likelihoods - AHC 150
5.9 Vulnerabilities and ease of exploits - AHC 151
5.10 Assessment of impacts - AHC 153
5.11 Risk determination - AHC 155
5.12 Risk treatment - AHC 157

5.13 Overview of the information security risk management - AHC 159
5.14 Description of roles - AHC 165
5.15 Information security objectives - AHC 167
5.16 Processes for monitoring and measurement - AHC 171
5.17 Plans for the internal audit - AHC 173
5.18 Agenda for the management review - AHC 174
5.19 Register of the nonconformity and corrective action - AHC 174
5.20 Register of the action for continual improvement - AHC 175
5.21 Post-analysis of the AHC's documents and records 177

6.1 Satisfying the requirements of the ISO/IEC 27001 187

A.1 Threat catalogue 208

B.1 Vulnerability catalogue 211

C.1 Statement of Applicability for the AHC Limited 214

List of Figures

1.1 Overview of the thesis structure 5

2.1 Information system functions 12
2.2 Phases in the systematic literature review 22
2.3 Mapping of the ISO/IEC 27001:2013 to the PDCA model 27
2.4 Comparison of the primary studies by fulfilment 34
2.5 Trend of the primary studies by publication 34
2.6 Distribution of primary studies 36

3.1 INFORMS meta-model 45
3.2 Actor 47
3.3 Asset 48
3.4 Constraint 50
3.5 Goal 51
3.6 Objective 52
3.7 Role graphical notation 54
3.8 Role 54
3.9 Task graphical notation 56
3.10 Task 56
3.11 Threat 57
3.12 Treatment 58
3.13 Vulnerability 59
3.14 Conduct relationship 60
3.15 Define relationship 60
3.16 Dependency relationship 61
3.17 Exploit relationship 61
3.18 Harm relationship 62
3.19 Impact relationship 62
3.20 Include relationship 63
3.21 Mitigate relationship 64

3.22 Restrict relationship 65
3.23 Satisfy relationship 65

4.1 INFORMS framework 67
4.2 Mapping of ISO/IEC 27001 to INFORMS 70
4.3 Workflow of INFORMS framework 72
4.4 UML activity digram notations 75
4.5 Awareness graphical notation 80
4.6 Communication graphical notation 82
4.7 Documented Information graphical notation 83
4.8 Outline of an Operational Viewpoint 85
4.9 Activity diagram of Actors Description View 86
4.10 Activity diagram of Constraints Specification View 88
4.11 Activity diagram of Asset Management View 89
4.12 Activity diagram of Goal Delivery View 91
4.13 Outline of a Technical Viewpoint 93
4.14 Activity diagram of information security risk management 94
4.15 Activity diagram of Identification of Threats View 95
4.16 Activity diagram of Identification of Vulnerabilities View 97
4.17 Activity diagram of Assessment of Impacts View 99
4.18 Activity diagram of Risk Determination View 105
4.19 Activity diagram of Risk Evaluation View 106
4.20 Activity diagram of Risk Treatment View 109
4.21 Activity diagram of Risk Acceptance View 111
4.22 Outline of a System Viewpoint 113
4.23 Activity diagram of Objectives Specification View 114
4.24 Outline of a Standard Viewpoint 116
4.25 Activity diagram of Monitoring and Measurement View 117
4.26 Activity diagram of Internal Audit View 119
4.27 Activity diagram of Management Review View 120
4.28 Activity diagram of Nonconformity and Corrective Action View . . . 122
4.29 Activity diagram of Continual Improvement View 123

5.1 Overview of the context and units of analysis 128
5.2 Operational Viewpoint - AHC 146
5.3 Technical Viewpoint - AHC 161
5.4 Objectives Specification View - AHC 168
5.5 Monitoring and Measurement View - AHC 170

5.6 Internal Audit View - AHC 172
5.7 Management Review View - AHC 174
5.8 Nonconformity and Corrective Action View - AHC 175
5.9 Continual Improvement View - AHC 175
5.10 Snapshot presentation of all views - AHC 179

Acronyms

AII Asset Impact Indicator. 100
ARI Asset Risk Indicator. 105
AURUM AUtomated Risk and Utility Management. 29

BSI British Standard Institution. 17

C2M2 Cybersecurity Capability Maturity Model. 15
CCSC Commercial Computer Security Centre. 17
COBIT Control Objectives for Information and Related Technologies. 13
CVE Common Vulnerabilities and Exposures. 189
CVSS Common Vulnerability Scoring System. 189

DTI Department of Trade and Industry. 17

GDPR General Data Protection Regulation. 1
GII Goal Impact Indicator. 100
GORE Goal-oriented Requirements Engineering. 7
GRI Goal Risk Indicator. 105

HeRA Heuristic Requirements Assistant. 29

I-SolFramework Integrated Solution Framework. 30
ICO Information Commissioner's Office. 46
IEC International Electrotechnical Commission. 2
INFORMS INtegratable Framework for mOdelling Requirements of Management Systems. 42
ISACA Information Systems Audit and Control Association. 13
ISM Information Security Management. 18
ISMS Information Security Management Systems. 2
ISO International Organisation for Standardisation. 2
ISSRM Information System Security Risk Management. 28
ITGI IT Governance Institute. 3

JTC Joint Technical Committee. 18

KAOS Keep All Objectives Satisfied. 8

NFR Non-Functional Requirements. 8

NHS National Health Service. 10

NIST National Institute of Standards and Technology. 95

PACTS PAttern-based method for establishing a Cloud specific informaTion Security management system. 31

PII Personally Identifiable Information. 127

PIMS Privacy Information Management System. 188

PRESS Peer Review of Electronic Search Strategies. 23

PrISM Preventive Information Security Management. 27

SCADA Supervisory Control and Data Acquisition. 30

SD Special Data. 127

SMP Security Management Platform. 30

SOX Sarbanes-Oxley. 12

SREP Security Requirements Engineering Process. 27

SREPPLine Security Requirements Engineering Process for Software Product Lines. 28

UML Unified Modeling Language. 44

Acknowledgements

The journey that has culminated with this thesis is far from an individual accomplishment. I wish to express profound thanks to the many people who have helped shape this work through their support and feedback.

I am privileged and deeply grateful for my two supervisors; many of the outcomes in this thesis have stemmed from stimulating meetings with them.

I would like to thank Professor Haralambos Mouratidis for the opportunity to collaborate with him, and his guidance on the research project has been greatly inspirational. I thoroughly enjoyed the supervision sessions, informative discussions and constructive advice in becoming a developing researcher.

I am ineffably indebted to Dr Saeed Malekshahi for his unwavering support, and his perceptive insight was unrivalled and enriched my efforts. His faith in my ability has been a constant source of encouragement and reassurance; my academic and professional development has flourished on account of his vast knowledge and generous input. This work would not have been possible without him.

This thesis also benefitted from invaluable comments and recommendations by my examiners, Professor Hamid Jahankhani and Dr Panagiotis Fotaris. Also, it has been a great honour to share these years with a wonderful cohort of fellow researchers and colleagues whose friendship I truly value.

And finally, I dedicate this work to my indefatigably supportive parents and sister for their endless love.

Declaration

I declare that the research contained in this thesis, unless otherwise formally indicated within the text, is the original work of the author. The thesis has not been previously submitted to this or any other university for a degree, and does not incorporate any material already submitted for a degree.

Signed

December 2019

Chapter 1

Introduction

In the new global economy, organisations face tougher pressure in securing the information of their clients. Some of these pressures are through mandatory rules and regulations, such as complying with the European Union General Data Protection Regulation (GDPR)[1], the interested parties' requirements, or safeguarding trade secret and commercial knowledge from their competitors. Increasingly, regulations demand software engineers analyse, design and implement responsible systems to comply with laws and regulations [1]. It is an essential task for organisations to meet their information security requirements and take appropriate actions to satisfy their expectations.

The number of information security breaches is getting bigger, and invaders are getting smarter in ways to exploit security vulnerabilities [2, 3]. Conventional and outdated management of security systems does not answer the needs of the current structure. According to Gartner, the business impact of security incidents and evolving regulations have led to information security spending growth [4]. Security services will continue to be the fastest-growing sector and particularly in IT outsourcing, consulting and implementation services. Improving security in an organisation is not just about expenditure on new technologies but correctly addressing the basics of information security and risk-related elements such as threat and vulnerability management, log management, backup and system hardening [4].

The continual change in technology, the use of technology and the impact on business success make the management information systems an exciting topic in business [5]. Experts believe that more than 90% of successful cyberattacks could have prevented by the technology available at the time [6]. The technology provides a foundation, but in the absence of intelligent management policies, even the best technology could be defeated.

[1] https://www.eugdpr.org/

To date, there has been no substantial evidence for absolute security and protection. However, there are available frameworks and approaches such as the International Organisation for Standardisation (ISO)[2] and the International Electrotechnical Commission (IEC)[3] 27001 standard[4] to promote the best practices in managing information security. Organisations need to prepare towards sophisticated approaches considering security techniques under one interconnected application known as Information Security Management Systems (ISMS) to preserve the confidentiality, integrity, and availability of information assets.

ISO/IEC 27001 is an international standard and applicable to all organisations, regardless of their type, size, or nature [7]. It constitutes a certifiable standard and is widely used with steady growth in adoptions [8]. The standard is composed of processes, policies, and resources used to systematise the security demands of an organisation. The ISO/IEC 27000 family of standards help organisations to implement a robust approach for managing information security and building resilience. By providing compliance to a globally known standard, certification significantly reduces the need for repeated client audits [9].

1.1 Motivation

IT Governance[5], a provider of IT compliance solutions to organisations released an annual survey [10] centred around the experience and implementation challenges of the ISO/IEC 27001 for organisations in 2016. The investigation of 250 information security professionals from 53 countries who participated in the survey was mostly certified or working towards certification (80%). 71% of respondents received either regular or occasional requests to provide the ISO/IEC 27001 certification from clients or when proposing for new business. By providing compliance to a globally known standard, certification significantly reduces the need for repeated client audits.

The survey also found that a third of all respondents were concerned about understanding the requirements of the standard and 28% considered the creation and managing the standard documentation a challenging task. Other substantial challenging tasks were conducting the information security risk assessment and identifying the required controls for 22% and 14% of the respondents, respectively.

Organisations can have substantial benefits from the implementation of information security; effective control and information system in place could have a solid

[2]ISO was set up in 1947 in Geneva, Switzerland with primary purpose is to develop standards that support and facilitate international trade.

[3]IEC established in 1906 in Geneva aiming to develop standards for all types of electrotechnologies.

[4]https://www.iso.org/isoiec-27001-information-security.html

[5]https://www.itgovernance.co.uk/

foundation for improvement in customer satisfaction, reputation, competitive position, sales and profitability [11]. A survey performed by IT Governance Institute (ITGI)[6] suggested a definite link between the effectiveness of IT governance and the frequency in which IT is discussed at the board level, the results indicate an improvement of IT performance, management of resources, and better risk management towards the organisation strategy [11].

Understanding and applying the requirements of any standard into an organisation is not always a straightforward process. From the review of the literature, it appears that opportunities exist to evaluate the implementation and effectiveness of the standard in organisations, but academic researchers as described in Chapter 2 have not taken the challenge. Our research proposes a model-driven framework to enable organisations to adopt the requirements of the standard using requirements engineering concepts.

Most system designers may not have sufficient expertise in security and legal aspects to protect and deploy systems to meet the security needs of an organisation. Therefore, a framework to guide them through the system development is suggested [12]. Implementation of information security management systems requires a comprehensive, well-planned process to identify the relevant assets and risks to the operation and well-being of the organisation. It is critical to understand the underlying notions of security in order to specify security requirements. A significant source of information security failures is the paltry consideration of the security requirements of the complete system [13].

Organisations understand that it is in their interest to follow recognised reference frameworks to create an environment for managing information security rather than doing it ad hoc [14]. From the commercial aspect, it is rather costly and challenging task to identify the resource required to plan, implement, measure information security management. From an academic perspective, ISMS has mostly drawn from the views of practitioners [15] and the investigation of the literature indicates that ISMS has not been particularly attractive in academia with a lack of research and approaches are egregious.

Management systems on information security have received minimal observation and research from the academic community despite the high interest from organisations in particular for IT, operational and compliance audits [16]. There is a relative paucity of scientific literature focusing specifically on the requirements of the standard; most of these studies have been on the previous version of the standard before 2013 [17]. In response to the real-world and academic challenges, this

[6]https://www.isaca.org/ITGI/Pages/default.aspx

thesis contributes a model-driven approach to organisations to identify, analyse, and implement the requirements of the standard.

1.2 Research Questions

In this section, we articulate our research questions to address the identified gaps in the literature. The main research questions formulated in this thesis can be stated as follows:

RQ.1 How to model the application of information security management system in an organisation using security requirements engineering concepts?

RQ.2 How to guide an organisation using a systematic process to implement information security management systems?

RQ.3 How to analyse the conformity of an organisation to the requirements of ISO/IEC 27001 Standard?

1.3 Aim and Objectives

The aim of this research is the *development of a set of concepts and processes to analyse and implement the requirements of the ISO/IEC 27001 Standard.*

This research intends to explore the standard in detail and determine what the available approaches are for organisations if they intend to adopt such a management system across their board. Our objectives to meet during this research are to:

RO.1 Identify and analyse the relationship between the requirements of the ISO/IEC 27001 Standard.

RO.2 Define a modelling language capable of modelling the requirements of the ISO/IEC 27001 Standard from a security requirements engineering perspective.

RO.3 Develop a framework to support the implementation of information security management systems in an organisational setting.

RO.4 Propose a method to address information security risk management per situational needs.

RO.5 Develop a process to analyse the effectiveness of information security management systems.

1.4 Thesis Structure

This thesis is conceptually structured using a bottom-up approach, as illustrated in Figure 1.1 in order to address our research questions, aim and objectives. The thesis organised in six chapters and each described below.

Chapter 1 delineates the introduction to the thesis, research questions, defining aim and objectives.

Chapter 2 expounds a systematic literature review which explores the scope of the research. It provides a thorough investigation of the gaps in the knowledge and summarising the related approaches. This chapter presents the research baselines used as part of the thesis.

Chapter 3 demonstrates our proposed modelling language. The chapter provides a detailed explanation of each concept introduced in the language and illustrates the relationships in the language's meta-model.

Chapter 4 presents the framework, its building blocks and their working relationships between each viewpoint and view.

Chapter 5 depicts a case study to evaluate the usability and effectiveness of the proposed language and framework. The chapter introduces the nature of the case study that follows the processes to utilise the framework. Finally, it provides a complete result of the evaluation.

Chapter 6 concludes the contributions of the research and provide suggestions for future research.

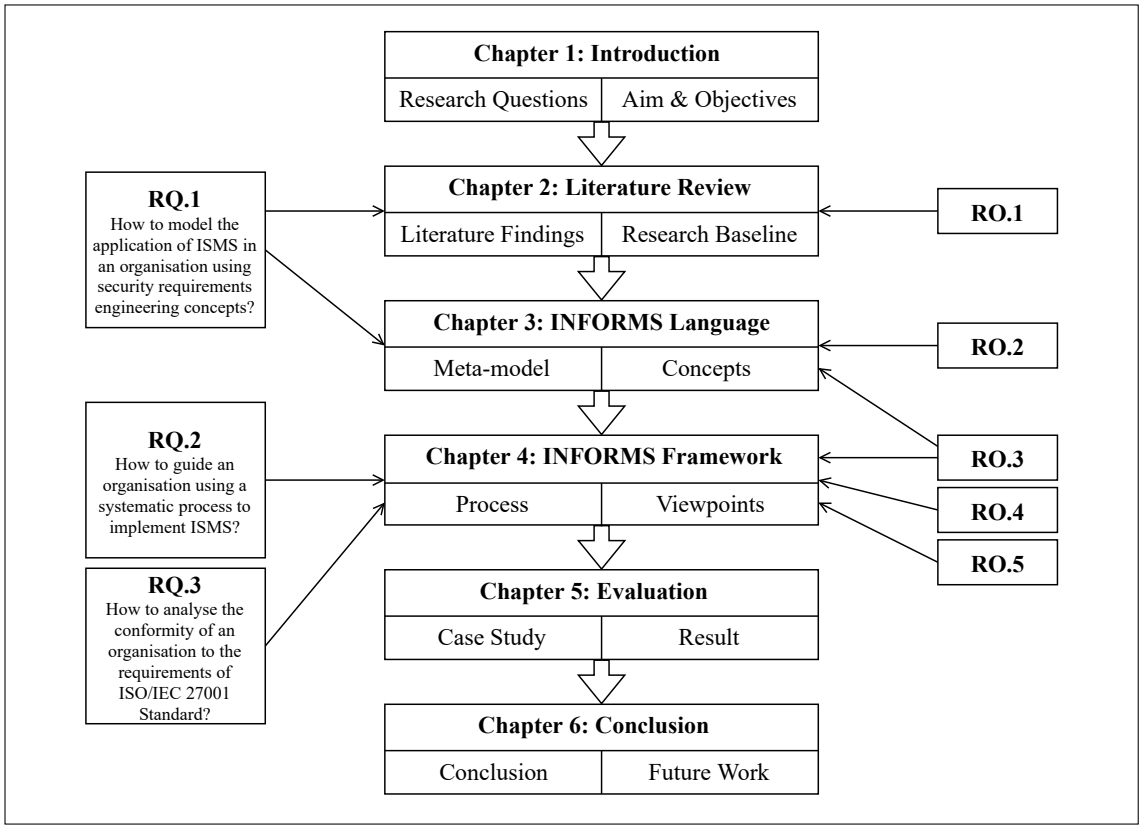


Figure 1.1: Overview of the thesis structure

Chapter 2

Literature Review

This chapter reviews the literature that surrounds the aim of the research. A vital purpose of this review is to synthesise the information collected by the literature in the area of information security management systems and identify current gaps and challenges. It begins by exploring the area of requirements engineering and widely used information security frameworks. Next, it systematically investigates the related work, draws together the essential findings and identifies the main challenges in the area of research. Finally, it establishes the research baselines by defining common attributes used throughout the research.

2.1 Background

The following subsections provide detailed analysis of the research background in the literature.

2.1.1 Requirements Engineering

This thesis focuses on bridging the work in software engineering with ISMS and align security requirements engineering towards the analysis and development of secure systems in organisations.

Requirements engineering is a coordinated set of activities for exploring, evaluating, documenting, consolidating, revising and adapting the objectives, capabilities constraints, assumptions that the system-to-be should meet based on problems raised by the system-as-is [18, 19]. Lamsweerde et al. [20] state a general issue with requirements engineers is their expectation of the first sketch of goals, requirements and assumptions are too exemplary; this likely to cause unexpected behaviour of agents such as human, devices or software components during the operation of the system. Authors proposed techniques to manage exceptions at requirements engineering and goal levels and providing formal techniques for resolving obstacles to the

satisfaction of goals, requirements and expectations expected in the requirements engineering process.

De Gea et al. [21] claim development team should be able to access requirements specification easily with traceability throughout the project life cycle. Authors categorised a series of capabilities in the current requirements engineering tools: requirements elicitation, requirements analysis, requirements specification, requirements verification and validation, requirements management, and other capabilities. The system security is a complex process and a structuring methodology is required to secure overall security of information systems, all security measures should concern: physical security, operating security, logical security, and telecommunication and network security [22].

Security requirements engineering is for the security team to build a group of parametrised reusable templates that is achievable by the requirements team to engineer security requirements to meet the necessary compliance [23]. Security is about preserving systems assets from harm due to various form of attacks that could be reached by the various attackers; it is critical to understand the underlying notions of security engineering and most importantly security itself in order to specify security requirements.

Pfleeger [24] states software engineers rarely equipped to build in security from scratch and it mainly looked at the near the end of development. One of the significant sources of system security failure is not considering the security requirements of the complete system [13].

We now expand on the approaches within requirements engineering, and security requirements engineering, including those starting from the early requirements stage with a visual language and modelling component.

i* [25, 26] is a highly influential agent-oriented framework in the field of requirements engineering and developed to capture the strategic interests of multiple agents in complex systems. i* defines two models corresponding to different levels of abstraction involving actors with strategic intentions; the strategic dependency model resents intentional concepts while the strategic rationale represents rational concepts. The model describes actors, sets of dependencies and the dependum; which can be a resource, task, goal or softgoal concept. The strategic rationale model refines the intentional elements of an actor inside their boundary through the means-end and task-decomposition links. Some other extensions of i* which support security concepts are [27, 28].

Goal-oriented Requirements Engineering (GORE) is an internationally recognised for goal-oriented modelling [29], which integrates the core concepts of i* [30]

and the Non-Functional Requirements (NFR) framework [31]. GORE offers a visual goal-modelling language with a clear separation between model concepts and their graphical representations. The modelling language supports qualitative and quantitative attributes, through contribution links with icons, numbers and text. The GORE syntax is based on the i* language, sharing common concepts such as actor, goal, resource and task. GORE diagram describes the high-level organisational business goals and non-functional requirements of stakeholders with alternative ways to achieve them.

GORE supports evaluations by analysing trade-offs between conflicting goals, through qualitative or quantitative satisfaction values. A strategy is the starting point of evaluations, given initial satisfaction values between intentional elements. Three directions of propagation are supported between linked intentional elements while taking contribution types into account, providing a global assessment of a system. The qualitative and quantitative attributes have the potential to support the refinement and selection of cloud services based on user needs.

Tropos is an agent-oriented software development methodology, focusing on the development life cycle from early requirements to implementation [32]. The Tropos modelling language is based on the i* framework, which describes models in Tropos through instances from the i* metamodel [33]. However, instead of defining types of models such as the strategic dependency and strategic rationale in i*, Tropos uses views to represent the different levels of abstraction between phases. The Tropos methodology has five development phases: early requirements, late requirements, architectural design, detailed design and implementation. Tropos focuses on the early and late requirements stages.

Keep All Objectives Satisfied (KAOS) [34] is a goal-oriented requirement engineering method to elaborate objectives to be achieved by the system-under-design into requirements and assumptions, where the responsibilities assigned to agents. The method focuses on the feasibility, completeness and consistency of requirements through a semi-formal graphical notation or formal when needed. In [35] van Lamsweerde consolidates research on KAOS to include formalisation of requirements using linear-time temporal logic in [36], analysis for conflicting requirements in [37], and the use of anti-models to elaborate security requirements in [38].

The KAOS method considers multiple stakeholders in a system-under-design and defines multiple views corresponding to different models. For example, in a goal model, stakeholder goals are refined through an "AND/OR" refinement tree. Again while the KAOS method allows refinement of goals to represent stakeholder needs, the language lacks the expressiveness to capture specific concepts.

So far, this section defined and motivated key requirements engineering approaches, capturing stakeholder and system requirements from an agent and goal-oriented perspective. Next, it describes work which extends these approaches to integrate security concepts through a security requirements engineering approach.

Security Requirements Engineering

Mellado et al. present a systematic literature review of existing work in security requirements engineering, providing state-of-the-art approaches in the field [39]. Their process identifies initiatives in work adapting a security requirements approach and focusing from the early stages of the software development life-cycle. Thus the authors' work motivates our review of security requirements engineering approaches which support modelling and reasoning about security requirements.

Fabian et al. propose a conceptual framework to consolidate central concepts used in security requirements engineering in [40]. They review a range of approaches including UML-based, goal-based, multilateral, problem frame-based, risk analysis-based and Common Criteria [1]. Authors provide a mapping between the diverse terminology to their proposed framework, providing specific approaches according to the scope of the issue.

STS-ml [41] is a security-oriented modelling language capturing the security requirements of multi-agent socio-technical systems. The approach focuses on describing the social interactions between social and technical actors in a system-to-be. It defines commitments to denote agents security needs, based on the satisfaction of security properties, such as non-disclosure of confidential data or non-repudiation of a delegated goal. While their approach tackles socio-technical systems based on social interaction between agents, it does not support a specialised vocabulary for capturing management system concepts.

Secure Tropos [42, 43] is a goal-oriented software engineering methodology extending the Tropos methodology to model security concerns throughout the software system development process, based on the notion of agents and related notions such as actor, goal, early analysis, and design stages. Mouratidis et al. present a framework to elicit the security and privacy requirements of software systems and define a modelling language as part of the process. The language extends from several concepts in the software engineering discipline, such as the i* framework, PriS [44] and Secure Tropos which provides specialisation in requirements engineering, privacy engineering and security engineering respectively [45].

Bandara et al. carry out a comparative evaluation of model-based security pat-

[1]The Common Criteria establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408, which in its entirety used as the basis for evaluation of security properties of IT products.

terns to examine the extent of support of constructs provided by security requirements engineering approaches. They cover three main categories of modelling approaches; design, goal-oriented requirements and problem-oriented. Their results suggest that "current approaches to security engineering are, to a large extent, capable of incorporating security analysis patterns" [46].

2.1.2 Information Security Frameworks

It is a critical task for organisations to meet their security expectations and take appropriate approaches to satisfy their requirements. Organisations face tighter pressure in securing their internal and external information. While there is no way to guarantee absolute security and protection but there are available standards and guidelines that promote the best practices in the management of information security.

In 2017, the UK National Health Service (NHS) was hit by one of the biggest ransomware[2] outbreak in the history called WannaCry[3]. The malware exploits a vulnerability in specific Microsoft Windows. A patch was released to fix the vulnerability much earlier to the incident; however, it was not installed and updated on the NHS computers to prevent the attack. The attack led to disruption in one-third of hospital trusts in England (80 out of 236), a further 603 primary care and other NHS organisations were infected by WannaCry, including 8% of GP practices (595 out of 7,454) [47].

Another infamous data breach which could be the largest hack of all time is that the 500 million user account credentials stolen from Yahoo[4] in 2014 and a different attack on the company in 2013 compromised more than one billion accounts including names, telephone numbers, date of birth, encrypted passwords and unencrypted security questions that could be used to reset passwords [48]. Organisations need to prepare toward more managed systems considering security and its associates under one interconnected application to successfully manage confidentiality, integrity, and availability of data.

Hackers are becoming increasingly innovative with the techniques they use to access sensitive data. Emerging technologies such as 5G networking may have many

[2]Ransomware or Ransom malware is a type of malicious software that infects and restricts access to a system or personal files until a ransom paid. One of the most common methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software.

[3]The WannaCry ransomware is a worm that spreads by exploiting vulnerabilities in the Windows operating system. It began to spread across computer networks in May 2017. WannaCry ransomware infects Windows computers, encrypting files on the hard drives of PCs so users could not access them and then demanded a ransom payment via bitcoin.

[4]https://www.yahoo.com

undiscovered new vulnerabilities for organisations by capitalising on people's lack of understanding of how these technologies work. Ericson projected that there will be more than 10 million 5G subscribers by the end of 2019. It includes cell phones, Internet of Things endpoints, and any other internet-enabled device capable of supporting 5G connectivity. This results in a substantial threefold increase in global mobile data traffic each month by the end of 2024 [49].

5G networks are the future backbone of our increasingly digitised economies and societies. Billions of connected systems are concerned, including in critical sectors such as energy, transport, banking, and health. Ensuring the security and resilience of 5G networks is therefore essential.

The data travelling through 5G networks could be as harmless as social media browsing, but it could also contain sensitive patient information or critical business analytics. Securing massive, continuous data transfers will require substantial efforts to secure and protect large swaths of information. Further, threats to availability and integrity of networks will become major security concerns, as well as increased exposure to attacks and more potential entry points for attackers [50].

The terms data, information, and system frequently used in computer science as well as in the business context; however, these terms have not always been used correctly to reflect their true meaning. "Data is facts about people, other subjects and events" [51]. Data could be manipulated through tabulation, addition, subtraction, division, or any other operation that leads to a greater understanding of a situation and processed to produce information. They are the raw material in the production of information, and raw data are rarely meaningful or useful as information [52].

Information is facts or conclusions that have to mean within a context. Information means data that shaped into a form which is meaningful and useful to human beings. For information to be useful, it must be relevant, complete, accurate, current and obtained economically [52]. The system is an array of components that work together to achieve a common goal or multiple goals by accepting input, processing it and producing output in an organised manner.

Information System consists of a computer-based set of hardware, software, and telecommunication components supported by people and procedures that work together to process data and turn it into useful information [51]. The information system has been designed to support decision making, coordinating, control, analysis, and visualisation in an organisation [52].

Figure 2.1 [52] illustrates functions of an information system which contains information about an organisation and its environment. Environmental actors such as customers, suppliers, competitors, stockholders, and regulatory agencies interact

with the organisation and its information systems. The organisation is a formal legal entity with internal rules and procedures that take resources from the environment and processes them to produce outputs.

The process is the conversion, manipulation, and analysis of raw input into a meaningful form usually to produce information; hence, while data are raw materials, information is output [5]. Input is the capture or collection of raw data from within the organisation or from its external environment for processing in an information system. Feedback is the output that is returned to the appropriate members of the organisation to help them evaluate the correct input. The output is the distribution of processed information to the people or the activities for which it will be used.

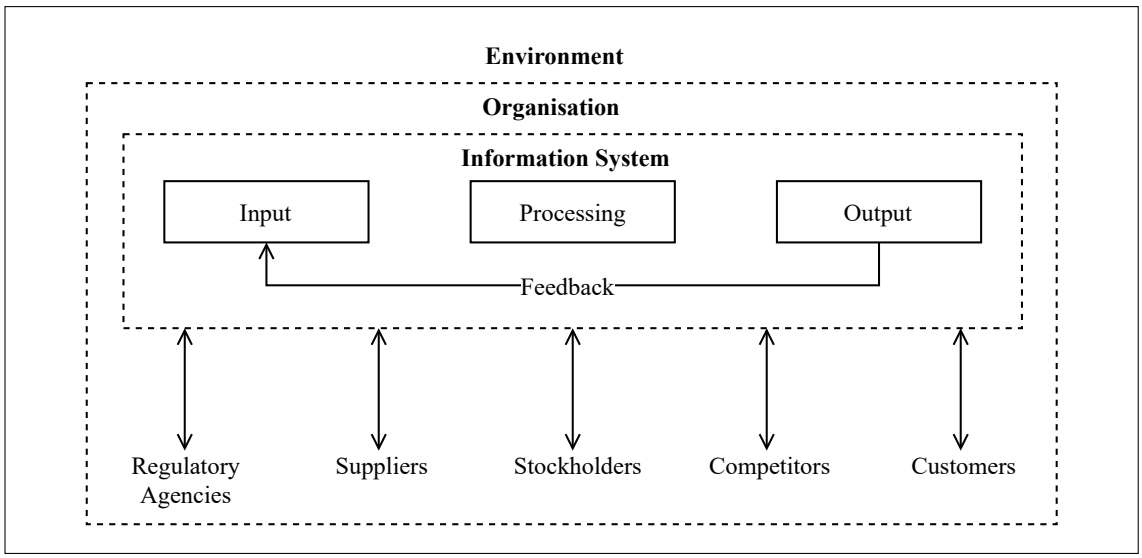


Figure 2.1: Information system functions [52]

It is speculated that most organisations produce information security policies derived from ISO/IEC 27000 family of standards or COBIT (see Section 2.1.2) if it is in the US, or mix and match controls from both or other relevant standards [53]. An organisation that publicly trade in the US is required to be comply with the requirements of Sarbanes-Oxley (SOX) Act[5] which specifically ask for information security policy and generally means COBIT controls; similar approaches applied in most countries.

Table 2.1 demonstrates a top-to-bottom approach of how laws, regulations and standards are interrelated and in partner together [53].

On the other hand, Siponen and Willison investigated the foundation of some of the normative information security management standards and reveals several weaknesses in the validity of these standards, some of these implications are discussed in [54]. The authors suggest that a standard should advocate a more reliable

[5]https://www.govinfo.gov/app/details/plaw-107publ204/related

development approach, such as research programs rather than an inductive method. Our proposed framework targeted national and industry standards and assists organisations in analysing and applying those standards.

Table 2.1: Top-to-bottom approach to IS standards and frameworks [53]

	USA	AU	EU	
National legislation	SOX	Privacy Act	EU GDPR	Legal
Industry regulation	PCI DSS	PCI DSS	PCI DSS	Legal
National standards	NIST SP 800-x	AS/NZS ISO 31000	ISO/IEC 27001	Security
Industry standards	ITIL, COBIT, OWASP			Business
Organisation	Information security policy			CSO, CIO

COBIT

Control Objectives for Information and Related Technologies (COBIT) delivers the latest integration of COBIT family developed by Information Systems Audit and Control Association (ISACA)[6]'s guidance on the enterprise governance and management of IT. It has developed through years of practical usage of COBIT by many organisations and users from business, IT, risk, security and assurance communities. It is used by IT professionals and increasingly by managers; internal and external auditors in the United States and other countries to align and manage the security of an organisation's information system [55]. The framework [56] is suitable for enterprises of all sizes and non-specific to any sector and structured in two areas that cover five domains and 37 processes as follow:

Area 1: Enterprise Goals – IT related Goals
- Evaluate, direct and monitor - 5 processes

Area 2: IT related Goals – IT related Process
- Align, plan and organise - 13 processes
- Build, acquire and implement - 10 processes
- Deliver, service and support - 6 processes
- Monitor, evaluate and assess - 3 processes

The COBIT 5 framework is specifically built to address five principles:

1. meeting stakeholder needs, the creation of value. Stakeholder needs drive realising benefits at an optimal resource cost while optimising risk;
2. covering the enterprise end-to-end, by merging governance of enterprise IT into enterprise governance;
3. applying a single integrated framework, which helps to align with other latest standards and frameworks and being overarching governance and management

[6]https://www.isaca.org/cobit

framework integrator;

4. enabling a holistic approach, categories of enablers that individually and collectively influence the governance of enterprise IT; and
5. separating governance from management, they comprise different types of activities with different responsibilities.

Wolden et al. [57] investigation of the effectiveness of COBIT in preventing risk on information systems found out that with correct direction of rules, responsibilities and policy, an organisation would benefit from averting and risk mitigation of a cyberattack. Authors indicate that top management is instrumental in the success of an information security system as well as a hierarchical structure within the organisation including employees and administrators have a direct influence on the implementation of such a framework.

Cybersecurity Framework

Cyber threats continue to grow and represent operational risks to organisations. Many organisations count the number of vulnerabilities and security breaches in a given period or report compliance with regulatory or industry standards to validate and measure their efforts. However, none of these approaches gives a true indication of an organisation's maturity, nor do they provide a framework for improvement.

Alternatively, organisations need to adopt a cybersecurity maturity model to measure and improve their cybersecurity. A cybersecurity framework provides a valuable approach to enable organisations to periodically assess and improve cybersecurity efforts.

NIST Cybersecurity Framework released in 2014 and developed in partnership with operators, academia, and the US Government to guide organisations within critical infrastructure sectors to reduce the risk associated with cybersecurity [58]. It is a comprehensive approach for measuring the organisation in the various domains covered to determine your level of maturity.

It is a framework for improving critical infrastructure through a set of activities designed to develop individual profiles to help owners and operators of the critical structure to identify, assess, and manage cyber risk. The Cybersecurity Framework consists of three main components of Tiers, Core, and Profile.

Tiers describe the implementation degree to which an organisation's cybersecurity risk management practices demonstrate the specification of the Framework. Organisations should determine the desired Tier, ensuring that the selected level meets organisational goals, reduces cybersecurity risk to levels acceptable to the organisation. The Tiers reflect a progression ranging from (Tier 1) Partial, (Tier 2) Risk-Informed, (Tier 3) Repeatable, and (Tier 4) Adaptive. Tiers do not necessarily

represent maturity levels.

The Cybersecurity Framework is a set of desired cybersecurity activities and outcomes organised into three parts including Functions, Categories, and Subcategories. The Framework Core is a non-technical language designed to be intuitive and to enable communication at the different operational levels. The Core includes five high-level functions:

1. Identify: organisational context to manage cybersecurity risk to systems, people, assets, data, and capabilities.
2. Protect: develop and implement safeguards to limit the impact of a potential cybersecurity event.
3. Detect: discovery cybersecurity events.
4. Respond: the ability to take action to contain the impact of a potential cybersecurity event.
5. Recover: recovery to normal operations to reduce the impact from a cybersecurity incident.

The five functions together have 23 categories that are not only applicable to cybersecurity risk management but also to risk management at large. The Categories were designed to cover the breadth of cybersecurity objectives for an organisation, while not being overly detailed. It covers topics across cyber, physical, and personnel, with a focus on business outcomes.

Subcategories are the deepest level of abstraction in the Core. There are 108 Subcategories, which are outcome-driven statements that provide risk-based considerations for creating or improving a cybersecurity program customised to the organisation's needs.

Profiles optimise the Cybersecurity Framework by delivering gap analysis to create a prioritised implementation plan suitable to the needs of the organisation. Profiles can be used to conduct self-assessments and identify opportunities for improving cybersecurity posture by comparing a current state with a target state of the cybersecurity. The current profile can be used to support the measurement of progress toward the target profile.

Cybersecurity Capability Maturity Model

The Cybersecurity Capability Maturity Model (C2M2) program was established by the U.S. Department of Energy under a public-private partnership effort to improve electricity subsector cybersecurity capabilities and to understand the cybersecurity posture of the grid [59].

A maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. Model content

typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline. A maturity model thus provides a benchmark against which an organisation can evaluate the current level of capability of its practices, processes, and methods and set goals and priorities for improvement. Organisations can benchmark their performance against other organisations.

The model focuses on the implementation and management of cybersecurity practices associated with the information technology and operations technology assets. It is publicly available and helps organisations to evaluate, prioritize, and enhance their cybersecurity capabilities. The C2M2 is presented at a high level of abstraction and provides descriptive guidance, which, it can be interpreted by organisations of various types, structures, sizes, and industries. It is based on a combination of existing cybersecurity standards, frameworks, programs, and initiatives.

The Electricity Subsector C2M2 and Oil and Natural Gas Subsector C2M2 models are energy sector-specific adaptation that includes the core C2M2 as well as additional reference material and implementation guidance specifically tailored for the aforesaid sectors.

The goal is to support ongoing development and measurement of cybersecurity resilience by strengthening organisations' cybersecurity and enables organisations to effectively and consistently evaluate and benchmark cybersecurity capabilities. Share knowledge, best practices, and relevant references across organisations as a means to improve cybersecurity posture.

This model consists of the following 10 domains, providing a measurement for each one to help organisations identify areas of weakness and strength. Each of the model's domains contains a structured set of cybersecurity practices. Each set of practices represents the activities an organisation can perform to establish and mature capability in the domain. The practices within each domain are organised into objectives, which represent achievements that support the domain. A brief description of the domains includes:

1. Risk management: identify, analyse, and mitigate cybersecurity risk to the organisation.
2. Asset, change, and configuration management: manage the organisation's IT and operations technology assets, including both hardware and software.
3. Identify and access management: create and manage identities for entities that may be granted logical or physical access to the assets.
4. Threat and vulnerability management: plans, procedures, and technologies to detect, identify, analyse, manage, and respond to cybersecurity threats and

vulnerabilities.

5. Situational awareness: activities and technologies to collect, analyse, alarm, present, and use operational and cybersecurity information.
6. Information sharing and communications: relationships with internal and external entities to collect and provide cybersecurity information to reduce risks and to increase operational resilience.
7. Event and incident response, continuity of operations: plans, procedures, and technologies to detect, analyse, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event.
8. Supply chain and external dependencies management: controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities.
9. Workforce management: plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel.
10. cybersecurity program management: an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organisation's cybersecurity activities in a manner that aligns cybersecurity objectives.

The C2M2 is a self-evaluation methodology and toolkit for an organisation to measure and improve its cybersecurity program. C2M2 uses a scale of Maturity Indicator Levels (MILs) 0 – 3 to measure progression.

The maturity indicator levels apply independently to each domain. As a result, an organisation using the model may be operating at different MIL ratings for different domains. The MILs are cumulative within each domain; an organisation must perform all of the practices in that level and its predecessor level(s) to earn a MIL in a given domain.

The model supports the implementation of the NIST Cybersecurity Framework. C2M2 Maturity Indicator Levels can be compared to the NIST Cybersecurity Framework Tiers.

ISO/IEC 27001 Standard

Department of Trade and Industry (DTI) Commercial Computer Security Centre (CCSC) established a set of internationally recognised security evaluation criteria and a code of good security practice in 1989. British Standard Institution (BSI) further developed this to British Standard BS7799-1:1995 Part 1: Code of Practice. In 1999, BSI revised BS7799-1 Part 1: Code of Practice and developed BS7799-2 Part2: Management System [60].

BS7799-1 Part 1: Code of Practice was adopted by ISO as ISO/IEC 17799:2000

Code of Practice for Information Security Management (ISM) in 2000. In 2005, ISO revised ISO/IEC 17799:2000 Part 1: Code of Practice to ISO/IEC 17799:2005 Code of Practice and reproduced BS7799-2:1999 Part 2: Management System to ISO/IEC 27001:2005 (Requirements). In 2007, ISO extended the ISO/IEC 17799:2005 Code of Practice for ISM to ISO/IEC 27002:2007 Code of Practice for ISM to provide practice recommendation and guidance as a reference for selecting controls within the process of implementing ISMS.

ISO/IEC 27001:2005 extensively revised in 2013, and it became generic with more flexibility, some controls were added or changed in the new document. ISO/IEC 27002:2013 revised the previously published edition in ISO/IEC 27002:2007.

National member bodies support both ISO and IEC, and they participate in the standards development process through technical committees. ISO/IEC 27001 standard is developed by the ISO/IEC Joint Technical Committee (JTC) 1, Subcommittee 27. JTC 1 is responsible for all kinds of information technology standards while Subcommittee 27 is specifically responsible for the development of standards related to IT security techniques.

ISO/IEC defined terms used in describing components of typical information security management systems to avoid confusion. These terms are often related to each other, and one term used in the definition of another term. ISO have grouped related terms to clarify relationships as well as defining their meaning. Definition of terms is a useful means of enabling the translation of the standards into other languages and assists auditors in their discussion with auditees. Terms and definitions for ISMS related standards and guidelines can be found in ISO/IEC 27000.

ISO/IEC 27000 family of standards help organisations to implement a robust approach to managing information security and building resilience. The ISO/IEC 27000 series of standards have been designed to be compatible with and complement other management systems such as ISO 9001 [7] and ISO/IEC 20000-1 [8]. Other documents in the 27000 family of standards provide guidance for various aspects of implementing and auditing ISMS, and there are also several standards giving sector-specific guidance.

Table 2.2 refers to published ISO/IEC 27000 family of standards related to "Information technology - security techniques". This is not an exhaustive list of pub-

[7]Quality Management System - This standard is based on a number of quality management principles including a strong customer focus, the motivation and implication of top management, the process approach and continual improvement.

[8]Service Management System - This document specifies requirements for an organisation to establish, implement, maintain and continually improve an IT service management system.

Table 2.2: ISO/IEC 27000 family of standards

Standard	Title
ISO/IEC 27000	Overview and vocabulary
ISO/IEC 27001	Requirements
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	Guidance
ISO/IEC 27004	Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC 27008	Guidelines for auditors on information security controls
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001
ISO/IEC 27010	Information security management for inter-sector and inter-organisational communications
ISO/IEC 27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000
ISO/IEC 27014	Governance of information security
ISO/IEC 27015	Information security management guidelines for financial services
ISO/IEC 27016	Information security management - Organizational economics
ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018	Code of practice for protection of personally identifiable information in public clouds
ISO/IEC 27019	Information security controls for the energy utility industry
ISO/IEC 27032	Guidelines for cybersecurity
ISO/IEC 27039	Selection, deployment and operations of intrusion detection and prevention systems
ISO/IEC 27040	Storage security
ISO/IEC 27043	Incident investigation principles and processes

lished ISO/IEC 27000 family of standards and only presents a selection of commonly referenced documents in the literature and industry.

The ISO/IEC 27001 technically refers to “Informational technology - security techniques - Information Security Management Systems - Requirements”. The current edition of ISO/IEC 27001 standard published in 2013 and specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation in order to conform with the standard.

Internationally recognised ISO/IEC 27001 is a comprehensive framework which

helps organisations manage and protect their information assets such as financial information, intellectual property, employee details. ISO/IEC 27001 includes a set of 114 controls split into 14 sections outlined in Annex A of the standard document. Also, the ISO/IEC 27002 is designed for organisations to use as a reference for selecting controls within the process of implementing an ISMS based on ISO/IEC 27001.

ISO [7] defines ISMS as a systematic approach to managing sensitive information so that it remains secure. It includes people, process and IT systems by applying a risk management process. The information security management system is composed of processes, policies, and resources used to systematise the security demands of an organisation. The framework helps to continually review and refine the security procedures in organisations to remain safe and secure.

The standard provide mapping for establishing, implementing, maintaining and continually improving an information security management system or alternatively known as Plan, Do, Check, Act (PDCA) model. It is a strategic decision for an organisation to adopt ISMS and to preserve the confidentiality, integrity, and availability of information by applying risk management process and giving confidence to interested parties that information security risks are adequately managed. The implementation of ISMS is influenced by their needs and objectives, security requirements, the process employed and the size and structure of the organisation. It is crucial that the ISMS is part of and integrated with the organisation's processes and overall management structure and that information security considered in the design of processes, information systems, and controls.

The standard developed containing many significant structural inter-related components. These components focus on normative references describing requirements for those seeking certification and conformity with ISO/IEC 27001. ISO does not perform certification or involve with issuing certificates.

Compliance with ISO/IEC 27001 can be formally assessed and certified by an external accredited certification body. ISO [61] defines certification as "the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements." An accreditation is "the formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards."

Leading benefits of ISO/IEC 27001 experienced by BSI [62] customers are 75% reduction in their business risk, 80% inspires trust in their business, 71% helps to protect their business. BSI describes that the standard can help small, medium, large businesses in any sector to keep information assets secure. Some organisations

choose to implement the standard in order to benefit from the best practices it contains, while others decide to get certified to reassure clients; for some industries, certification is a legal or a contractual requirement.

ISO performs a survey of valid certifications to management systems standards reported for each country annually. ISO [8] recorded a total of 1,654,523 certificates across nine standards in 2016 compared to 1,520,368 in 2015, an increase of 8%. The ISO 27001 had valid certificates of 33,290 with 21% increase from 27,536 in 2015.

Top five industrial sectors for ISO/IEC 27001 certificate in 2016 were information technology with 6,578 certificates, Other services with 1,432 certificates, transport, storage and communication with 401 certificates, electrical and optical equipment with 311 certificates, financial sector, real estate, renting with 250 certificates.

The breakdown of the worldwide total of ISO/IEC 27001 certificates in 2016 were Africa 224 certificates, Central/South America with 564 certificates, North America with 1,469 certificates, Europe with 12,532 certificates, East Asia with 14,704 certificates, Central/South Asia with 2,987 certificates, the Middle East with 810 certificates. Top five sites covered by ISO/IEC 27001 certificates in 2016 were Japan with 13,889 certificates, China with 3,411 certificates, India with 3,038 certificates, the United Kingdom with 3,006 certificates, Italy with 1,517 certificates.

2.2 Investigation of Related Work

The following sections include information regarding the investigation and analysis of the related work.

2.2.1 Review Protocol

A systematic review is critical to identify all published and unpublished evidence, select studies, assess the quality of selected studies, synthesise the findings from studies or reports in an unbiased way which allows to interpret the findings and present a balanced and impartial summary [63]. This study conducted in the form of a systematic literature review by employing Guidelines for Performing Systematic Literature Reviews in Software Engineering introduced by Kitchenham et al. [64, 65] and Webster et al. [66].

The review involved a series of activities divided into three phases shown in Figure 2.2. The steps in the review method documented below.

Planning: the initial step sketched the need for undertaking this review by considering all current information about ISO/IEC 27001 and software engineering thoroughly and impartially. The second step of the planning specified the research questions by considering the types and structure of the questions, as discussed in Section

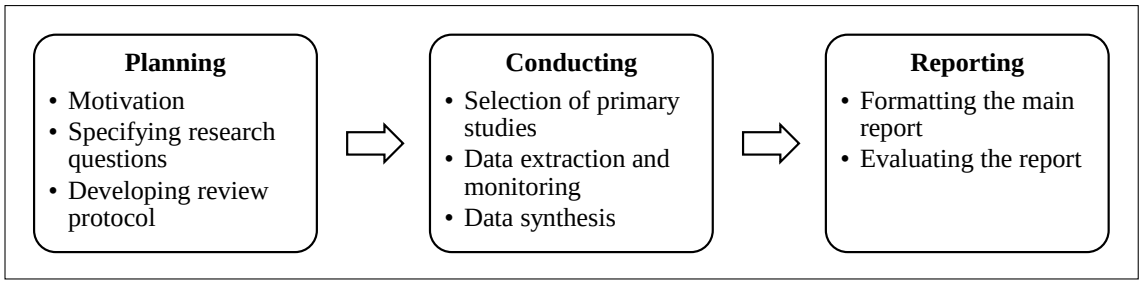


Figure 2.2: Summary of the phases in the systematic literature review

1.2. The last part of the planning phase developed a review protocol to specifies the methods used to undertake the review and reduce the possibility of bias. The components of our review protocol include study selection procedures, selection criteria, data extraction strategy, and synthesis of the extracted data explained in Section 2.2.1.

Conducting: this phase implemented the steps identified in the research protocol from the former phase. The initial step identified the primary studies which provide direct evidence about the research questions followed by accurately recording the information obtained from the primary studies. Finally, a descriptive synthesis of the primary studies developed to provide a summary of the results in Section 2.2.2.

Reporting: the last phase reported the review findings obtained from the results summarised in Section 2.2.3.

Search Process

A detailed inclusion and exclusion criteria governed the search and selection of the relevant papers. Each piece of literature reviewed and assessed by the researcher. An automated search strategy followed to identify the primary studies. The electronic libraries used included Google Scholar, IEEE Xplore, Springer, Science Direct, Research Gate, British Library EThOS, ACM Digital Library, Abstracts in New Technologies and Engineering, and Web of Science.

Specific keywords and synonyms established as part of searching for relevant concepts in the literature. A sophisticated search string constructed using Boolean ANDs and ORs for the retrieval in the digital libraries. The string given below derived and taken as a basis, which applied to the title, keywords, and abstracts of publications.

((“iso/iec 27001 standard” OR “information security management systems” OR “isms” OR “information security standard” OR “security standard”) AND (“requirements engineering” OR “compliance engineering” OR “security requirements engineering” OR “software engineering”))

The above search strings assessed and validated using the applicable elements

from the Peer Review of Electronic Search Strategies (PRESS) checklist [67]. The validation results obtained from the PRESS assessment set out in Table 2.3. Some electronic libraries did not provide advanced search options that allow for the use of the search string as-is. For these sites, the context of the search extended or separated the search into several sub-searches preserving the initial search context.

Table 2.3: PRESS checklist

PRESS Element	**Result**
Are the search concepts clear?	Yes
Are there any spelling errors?	No
Are any filters used appropriate for the topic?	Yes
Are any potentially helpful limits or filters missing?	No
Are there any mistakes in the use of Boolean or nesting?	No
Are the subject headings relevant?	Yes
Are the subject headings missing?	No
Are any subject headings too broad or too narrow?	No
Does the search miss any synonyms?	No
Does the full term include for the abbreviation used?	Yes
Does the search string match the research question?	Yes

Studies Selection

Peer-reviewed articles on the following topics included in the selection of studies, including:

- An article published between 01 Jan 2005 and 30 June 2018: we wanted to cover the years that both versions of the standard published in 2005 and 2013, hence, it is fair to cover from the start of 2005 until the current date.
- An article should discuss the search string described in Section 2.2.1.
- An article should propose a software engineering technique in addressing the standard: this thesis aims to capture the contributions from the field of software engineering.

Articles on the following topics excluded from the selection of studies, including:

- An article that is not written in English.
- White papers or informal articles: not peer-reviewed papers or articles which provide a plain description of the standard rather than purposing a technicality were excluded.
- Duplicate reports of the same study: when several reports of a study exist in different journals the most complete version of the study was included in the review.

Studies Extraction

This review does not claim to have captured every approach within the ISMS; however, it aims to have a holistic comprehension of the current state of the art in the ISMS. We recognise there could be some other related approaches that consider other ISMS methodologies such as COBIT, however, the intention of this thesis is ISO/IEC 27001 and to achieve a reasonably detailed conclusion within this topic.

The information extracted from the selected studies must reflect our research questions and indicates a desirable contribution toward the ISO/IEC 27001. The initial studies of 285 papers converged by learning their meta-data including title, abstract, keywords, and conclusion. A total of 95 papers met the aims of this review, which led us to investigate the full text of a study further. Finally, 21 papers selected as primary studies for in-depth evaluation.

The order of reporting the primary studies is in chronological order, and for fairness and accuracy, the same amount of information extracted from each selected study. The information elicited from each study are:

Approach title: proposed title by the authors for their contribution. If a title was not available, then the first author's full name used to refer to the study.

Year of publication: if a paper published in several different sources, both dates recorded and the first date used in any analysis.

Type: primary studies categorised into two terminologies including Framework or Method, the definition used for each listed below.

- Framework: process or layered conceptual structure intended to serve as a support or guideline for the building of something useful [68].
- Method: it refers to the methods the researchers use to perform an operation [69].

Scope: the contribution of each study was equally measured toward the PDCA model. The four stages include:

- Plan: establish the ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security.
- Do: implement and operate the ISMS policy, controls, process and procedures.
- Check: assess and measure process performance against ISMS policy.
- Act: maintain and improve the ISMS by taking corrective actions where non-conformity occurs.

Findings and practical implications: it refers to the analysis, discussion, results, and identification of outcomes and implications for practice in the primary studies. In the case of duplicate publications, the most completed paper used by referring to the versions of the report to obtain all the necessary information.

Studies Analysis

The standard specifies the requirements for establishing, implementing, maintaining and continually improving ISMS within the context of the organisation. Excluding any of the clauses of the standard is not permitted when an organisation wish to claim conformity to the standard; hence, this systematic review used a similar approach to measure the level of fulfilment to the requirements of the standard by each study.

A set of 22 criteria listed below excerpted from the clauses and sub-clauses of the ISO/IEC 27001:2013 [70] to compare and evaluate the studies. The review followed the same definition for each criterion as specified in the requirements of the standard to establish a uniform description; it avoids misinterpretation or misjudgement during the review process. The criteria selected from the current version of the standard published in 2013, however, it is recognised that the majority of the literature published before 2013. Therefore, a formal mapping [71] of ISO/IEC 27001:2013 clauses to ISO/IEC 27001:2005 version used to ensure that articles produced before 2013 are not disadvantaged in comparison with those introduced post-2013.

Figure 2.3 illustrates the mapping between the requirements of the ISO/IEC 27001:2013 and the PDCA model. The order in presenting the criteria do not reflect their importance or imply their implementing order, the list items enumerated for reference purpose only.

1. Organisational context: define the external and internal parameters and issues affecting the outcome of ISMS.
2. Interested parties: identify the interested parties and their information security requirements relevant to the ISMS.
3. Determining the scope: identify the logical or physical boundaries and applicability of the ISMS.
4. ISMS: establish, implement, and continually improve an ISMS under the requirements of the standard.
5. Leadership: top management to demonstrate leadership and commitment concerning the ISMS that are compatible with the strategic direction of the organisation.
6. Policy: establish directions and making references to information security objectives and appropriate to the purpose and context of the organisation.
7. Roles: top management to assign and communicate the responsibilities and authorities relevant to information security for reporting performance of the ISMS within the organisation.
8. Risks and opportunities: systematically determine the potential risks and op-

portunities that may be involved in a projected activity or undertaking.

9. Information security objectives: define measurable information security objectives.
10. Resources: identify the resources needs to manage the ISMS.
11. Competence: identify the necessary ability of a person's knowledge and skills doing work under its control that affects information security performance.
12. Awareness: personnel work under the organisation's control to be aware of the information security policy and their contribution to the effectiveness of the ISMS.
13. Communication: apply internal and external communication process relevant to the ISMS.
14. Documented information: create, update, and control documented information required by the standard and necessary for the effectiveness of the ISMS.
15. Operational planning: plan, implement and control the process needed to meet information security requirements including risk and opportunities, and information security objectives.
16. Information security risk assessment: perform information security risk assessment.
17. Information security risk treatment: implement information security risk treatment.
18. Monitoring, measurement, analysis and evaluation: evaluate information security performance and its effectiveness.
19. Internal audit: conduct regular internal audits and systematically evaluate the effectiveness of the implemented and maintained ISMS.
20. Management review: top management to review the organisation ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness.
21. Nonconformity and corrective action: react and evaluate nonconformity occurrences, review and deal with appropriate corrective actions.
22. Continual improvement: recurring activity to continually improve the suitability, adequacy and effectiveness of the ISMS.

2.2.2 Results

The following summarises the result of our review from the selected studies under the keywords that this thesis interested to investigate.

Chang and Ho proposed a model [72, 73] to explore the influence of organisational

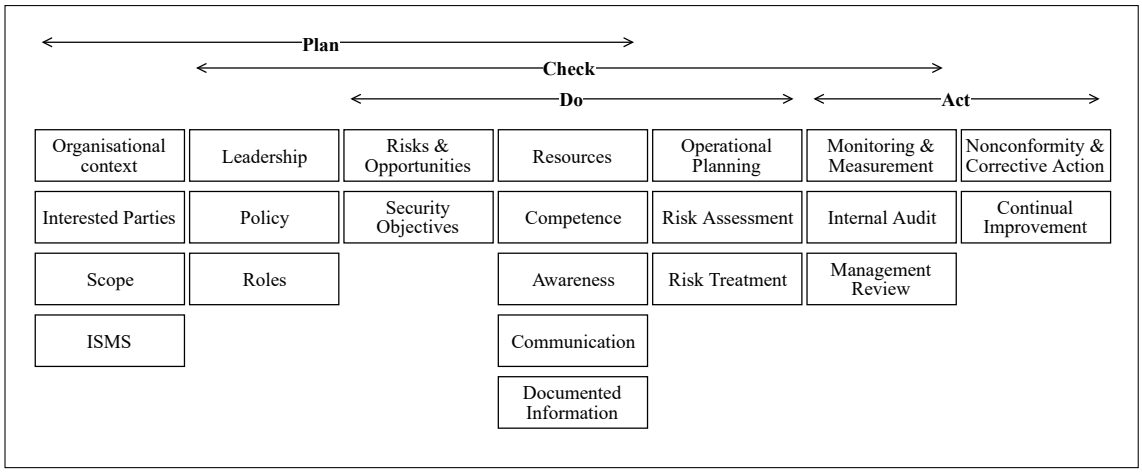


Figure 2.3: Mapping of the ISO/IEC 27001:2013 to the PDCA model

factors on the effectiveness of implementing the BS7799 [9]. The findings defined four factors that have a severe impact on the success of the implementation of the information security management; it included IT competence of business managers, environmental uncertainty, industry type, and organisational size. The impact of these factors varies between any types of organisations. The findings indicate that large organisations may benefit more in implementing information system security standards since they are more depended on formalisation and standardisation than small companies and have a more significant amount of assets. Their studies were limited as only targeted 59 organisations in Taiwan; however, the authors expect to have a similar result for another region too.

Mellado et al. proposed the Security Requirements Engineering Process (SREP) [74, 75], which incorporated security requirements such as Common Criteria into the software life cycle model in a structured process. SREP used a collection of standards, processes and activities for the development of secure information systems under a systematic approach. The framework made up of nine activities known as micro-process to form the security requirements engineering, as well as the external and visible artefacts that involve the activities. The activities included the determination of the security vision, understanding of the stakeholders, the identification of the vulnerabilities and assets, identification of security objectives and threats, risk assessment, the elicitation-prioritisation-inspection of security requirements and the repository improvement.

Anwar et al. proposed Preventive Information Security Management (PrISM) [76] system to model the security assurance and risk handling process in ISMS. PrISM developed a network security solution which included many services and func-

[9] replaced by ISO/IEC 27001 standard

tionalities, such as intrusion, detection and prevention capability, integrity checks, incident management and managerial reporting. The functions incorporated in a single control panel to enable the integration, summarising and linking all the tools and functionalities together. It assists with automating incident handling and other tasks, which ultimately could minimise the operational risks within organisations using comprehensive security monitoring.

Fenz et al. proposed OntoWorks [77, 78], an ontological mapping of the ISO/IEC 27001 supporting the certification process. Authors proposed a framework to use ontological data and enable users to access, visualise, and reason on ontological data. Their contribution helped for audit preparation and rule-based compliance checks regarding ISO/IEC 27001 controls. As some of the operations delivered as partial automation, this will increase the automation process within the certification process, resulting in saving costs and resources. Fenz et al. [79] later proposed security ontology used to increase the efficiency of the compliance checking process by introducing a formal representation of the ISO/IEC 27002.

Mellado et al. proposed Security Requirements Engineering Process for Software Product Lines (SREPPLine) [80, 81], a solution for managing security requirements at an early stage of the product line development driven by security standards. The framework structured management of the security requirements to facilitate the conformance of the software product line products to relevant security standards, e.g., ISO/IEC 27001 and ISO/IEC 15408. The proposal consisted of two sub-process including the product line security domain engineering and the product line security application requirements engineering. These sub-processes are responsible for four phases of requirements engineering, such as requirements elicitation, requirements analysis and negotiation, requirements documentation, and requirements validation and verification. Mellado et al. [82] later used Secure Tropos framework for Software Product Lines requirements engineering for elicitation of security requirements and analysis on both a social and technical dimensions.

Boehmer proposed a methodology [83, 84] to measure the effectiveness of the implementation and operation of ISMS in organisations. The methodology delivered an assessment solution through audits checking of the internal controls. Internal controls included administrative controls, physical controls, and technical controls.

Mayer proposed Information System Security Risk Management (ISSRM) [85, 86, 87], which provide a reference conceptual model for security risk management. The author proposed a model-based approach for ISSRM, applicable since the early phases of IS development. The work focused on the modelling support to such an approach by proposing a domain model for ISSRM. The work defined a concep-

tual reference model for security risk management and enhancement of the domain model with the different metrics used in a risk management method. Further, the author developed a proposal of the Secure Tropos language and a process to use the extension in the frame of risk management.

Ekelhart et al. proposed AUtomated Risk and Utility Management (AURUM) [88, 89], a risk management methodology to support the NIST 800-30 risk management standard. The methodology focused on the risk management approach by conducting various techniques such as questionnaires, on-site interviews, document reviews, and automated scanning tools to gather the required information under an ontological framework. AURUM provides risks assessment management by understanding the organisation characterisation modelled and taken from best practise standards such as the IT Grundschutz. It is a methodology for supporting information security risk management through modelling organisations' assets within an ontological framework.

Valdevit et al. proposed an approach [90, 91] on how to adopt ISO 27001 on SMEs and their specific needs in implementing ISMS. Authors described their approach as a "blend of theoretical reviews and experiments" developed by the knowledge gained in SMEs for several years in many disciplines and sectors. It is a method where researchers and practitioners work together towards several activities, including problem diagnosis, active intervention, and reflective learning.

Hensel and Lemke-Rust proposed an approach [92] of Braun [93] to business engineering chosen for the integration of ISO/IEC 27001 into an enterprise architecture. Authors integrated ISMS into systematic business engineering. The approach consisted of four layers such as strategic layer which considered the internal and external requirements of an organisation and its strategic alignment; organisation layer considered the overall organisation process vision and defined the roles and responsibilities of the ISMS; the information system layer considered the information assets and information architecture of the organisation; infrastructure and technology layer considered the infrastructure used for conducting a risk analysis of ISMS.

Schneider et al. proposed Heuristic Requirements Assistant (HeRA) [94], an assistant tool to enable the identification and analysis of security requirements by applying experience-based tool rather than dependency on experts. It provides knowledge about security best practises to developers and designers with limited experience; based on modelling the flow and enabling the stakeholders to exchange, learning and reusing relevant experiences about security requirements at the project requirements level.

Muller et al. introduced Security Management Platform (SMP) [95, 96], a tool to support cloud service providers and consumers. The platform specifies the security requirements and measures the effectiveness of implemented controls for cloud service providers and consumers to conjointly manage information security. The system management platform consisted of three steps: security requirements for a cloud service and its underlying infrastructure, the service provider manages the implementation and operation of identified controls, and service provider measures and analyses the effectiveness of controls identified in the first step.

Gillies proposed 5S2IS [97] to facilitates SMEs to implement and comply with the ISO/IEC 27000. The proposed approach developed a two-dimensional matrix with the use of the standard and the Capability Maturity Model (CMM). It included draw up a plan to understand the organisation expectation and achieve the ISMS, define policies and processes to reach the organisation goals, identify the non-compliances with the goals through measurement, analyse and identify the growth and improvement of performance through monitoring, embed the ISMS in the organisation and plan to attain for certification if applicable.

Susanto et al. proposed Integrated Solution Framework (I-SolFramework) [98, 99, 100] to assess the readiness level of organisations towards the implementation of ISO 27001. The framework offered e-assessment and e-monitoring to analyse and perform an assessment of the readiness level of ISO/IEC 27001 implementation. E-assessment measure ISO/IEC 27001 parameters based on the framework consisted of six layers component including organisation, stakeholder, tools and technology, policy, culture, and knowledge. It helped to validate the ISO/IEC 27001 parameters through an analytical interface such as histogram, charts and graphs, provided by a framework.

Montesino et al. proposed Security Information and Event Management (SIEM) [101], a framework to enable organisations to evaluate their compliance with information security standards and their implementation effectiveness by automatically generating ISO/IEC 27001 based on IT security metrics [102]. Authors findings indicated about 30% of the security controls of ISO/IEC 27001 could be automated. SIEM technology consisted of two main functions of a security information management system and security event management together to centralise and incorporate a list of ten automated controls.

Azuwa et al. proposed Supervisory Control and Data Acquisition (SCADA) [103, 104], an approach to measure the effectiveness of network security management in SCADA. This method specifically assisted in enabling a measurement approach to the effectiveness of ISO/IEC 27004. It initially identifies security controls

followed by a risk management approach to develop risk-based requirements and prioritisation of security control implementation. This step included the identification of threats and vulnerabilities and their impacts. The third stage to develop an effective measurement and metric through questionnaires and interviews, perception and experts' knowledge.

Beckers et al. proposed a methodology [105, 106] to analyse security requirements engineering methods to support the development and documentation of ISMS according to ISO/IEC 27001. Authors described the aims to improve the result of ISO 27001 implementation through proper establishment and documentation of ISMS.

Chatzipoulidis et al. proposed a risk management approach [107] called "to be" environment by focusing on analysing threats, evaluating and treating vulnerabilities in the information society. The author described information society as a dynamic information security management system and proposed a concept to enhance the role of e-government to support public administration and cognitive resource for policymakers. The "to be" environment methodology identifies risks by characterising the elements of risks and summarising critical threats of cyberbullying and cyberstalking attack patterns; identification of risk by analysing cultural dynamics and assessment of the current and planned controls of the system in place; evaluation of risk by producing a list of critical risks prioritised based on set criteria, and risk treatment to lessen risks to meet the risk appetite level.

Asosheh et al. proposed a framework [108] to assist large-scale enterprises in identifying related activities in establishing and implementing an ISMS including the risk assessment and treatment procedures. The process consisted of five steps according to ISO/IEC 27003 implementation guidance such as obtaining management approval for initiating the ISMS project. The steps included a preliminary scope identification and preparing definitions for ISMS and a business plan to have the management approval, defining ISMS scope, boundaries and ISMS policy, conducting information security requirements analysis, and risk management.

Beckers et al. proposed PAttern-based method for establishing a Cloud specific informaTion Security management system (PACTS) [109, 110, 111, 112], an approach to create ISMS methodology compliance to the ISO/IEC 27001 cloud environment with a specific interest in legal compliance and privacy. The overview of the methodology includes leadership commitment, asset identification, threats analysis, risk assessment, security policies and reasoning, ISMS specification, identify relevant laws and regulations, the definition of compliance controls, instantiating privacy patterns, and privacy threats analysis.

Beckers et al. proposed ISMS-CORAS [113, 114], an extension of the COROS

method to support the establishment of the ISO/IEC 27001. CORAS is a risk management methodology providing compliance to ISO 31000, and consideration of legal concerns tool support for document generation.

2.2.3 Discussion

In this section, we discuss the result of our systematic literature review to allow us to identify the gap in the knowledge and identify opportunities to achieve our aim and objectives as described in Section 1.3.

A description of each primary study narrated in the previous section, and in here we provide an overall description of the primary studies shown in Table 2.4, where appending each study Title, Year of publication, Type of contribution, Scope(s) of the PDCA model, and depth of fulfilment at each stage of the Plan, Do, Check, and Act.

Our speculation to the PDCA model is that very little attention given at the Check stage, which only five out of 21 studies contributed to the relevant part of the standard. Check deals explicitly with assessment and measurement process performance against the ISMS. Act stage tends to have less to almost no contribution, where only one out of 21 studies addressed the relevant part of the standard. Act maintains and improves ISMS by taking corrective actions where nonconformities occur. Interestingly, even some of the proficient concepts like ISMS-CORAS or ISSRM did not target any of the named stages of the standard in their studies.

The chart in Figure 2.4 depicts the overall fulfilment percentage of each study towards the requirements of the standard in chronological order from 2005 to 2018. This review provides evidence concerning a gap in the field of the ISMS.

The trend indicates that the current studies are fragmented, and it is a challenging task for organisations to benefit from the current literature. Hence, they require to apply several studies in conjunction with each other in which the outcome could be inconsistent, unmanageable, and intractable. While the existing literature could help with somewhat smaller sections of the standard and used as a point of reference but they are inadequate to realise the full requirements of the standard. Our findings suggest that the majority of studies proposed between 2005 to 2018 are incomplete and they mostly provide a partial fulfilment to the requirements of the ISO/IEC 27001.

The graph in Figure 2.5 reveals that a reasonable quantity of the studies produced between 2006-2008, after the publication of the first version of the standard in 2005; the attention dropped until around 2010. Half of the studies carried out between 2011 to 2013 and it appears the consideration to the ISMS was higher before the

Table 2.4: Overall description of primary studies

Title	Year	Type	Plan	Do	Check	Act
Chang, Shuchih Ernest	2006	M	+	-	-	-
SREP	2007	F	+	+	-	-
PrISM	2007	M	-	-	+++	++
OntoWorks	2007	F	-	+	++	-
SREPPLine	2008	F	++	+	-	-
Boehmer, Wolfgang	2008	M	+	+	-	-
ISSRM	2008	M	++	+++	+	-
AURUM	2009	M	+	++	-	-
Valdevit, Thierry	2009	M	+	-	-	-
Hensel, Veselina	2010	M	+	++	-	-
HeRA	2011	M	+	-	-	-
SMP	2011	F	+	-	++	-
5S2IS	2011	F	+	+	++	-
I-SolFramework	2012	F	++	-	-	-
SIEM	2012	F	-	+++	-	-
SCADA	2012	M	-	++	-	-
Beckers, Kristian	2012	M	+	+	-	-
“to be” environment	2013	M	+	++	-	-
Asosheh, Abbass	2013	M	+	+++	-	-
PACTS	2013	M	++	++	-	-
ISMS-CORAS	2013	F	++	+++	-	-

Note:
F = Framework
M = Method
- = Not fulfilled
+ = Partially fulfilled = Number of criteria per scope: Plan [1-5], Do [1], Check [1], Act [1]
++ = Mostly fulfilled = Number of criteria per scope: Plan [6-10], Do [2], Check [2], Act [1]
+++ = Fulfilled = Number of criteria per scope: Plan [11-14], Do [3], Check [3], Act [2]

publication of the second version of the standard in 2013 than after. This shows an inconsistent and contradicts association between the first version and the second version of the standard. A possible explanation could be the fact that other standard documents in the family of ISO/IEC 27000 were revised and published between 2011-2013, such as a revised publication of ISO/IEC 27003 in 2010, ISO/IEC 2005 in 2011, ISO/IEC 27006 in 2011, ISO/IEC 27007 in 2011, ISO/IEC 27008 in 2011.

The most striking result to emerge from the data is that the expansion of further research dropped sharply after 2013 and no study detected after the revised publication of the standard in 2013, which should have caused some spark in academia. It

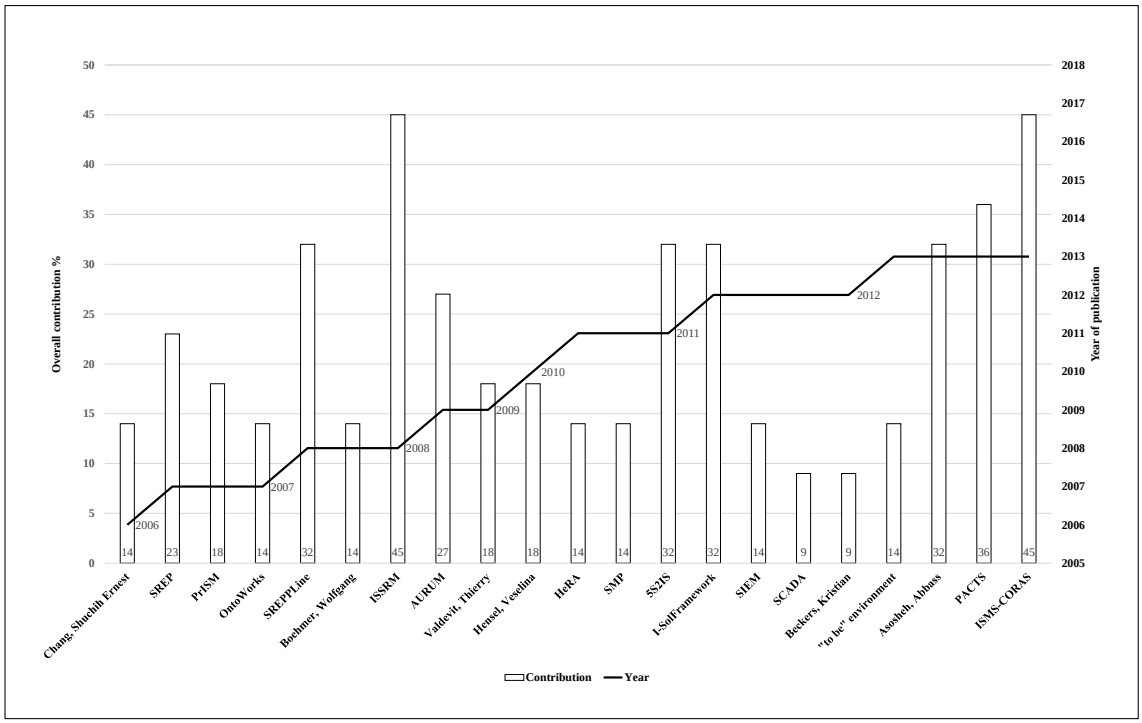


Figure 2.4: Comparison of the primary studies by fulfilment in (%)

is interesting to note that almost all papers (20) published between 2007 to 2013.

Table 2.5 demonstrates a detailed review of all 21 studies and their contribution at each criterion identified in the previous section; It provides the overall strength and limitation of the study. The indicative (+) sign in the table denotes the fulfilment of a criterion.

On average, some criteria are shown to have attracted the majority of the literature than others. The areas where significant differences found include Organisational context (1), Interested parties (2), Determining the scope (3), Documented information (14), Operational planning (15), and Information security risk assessment (16).

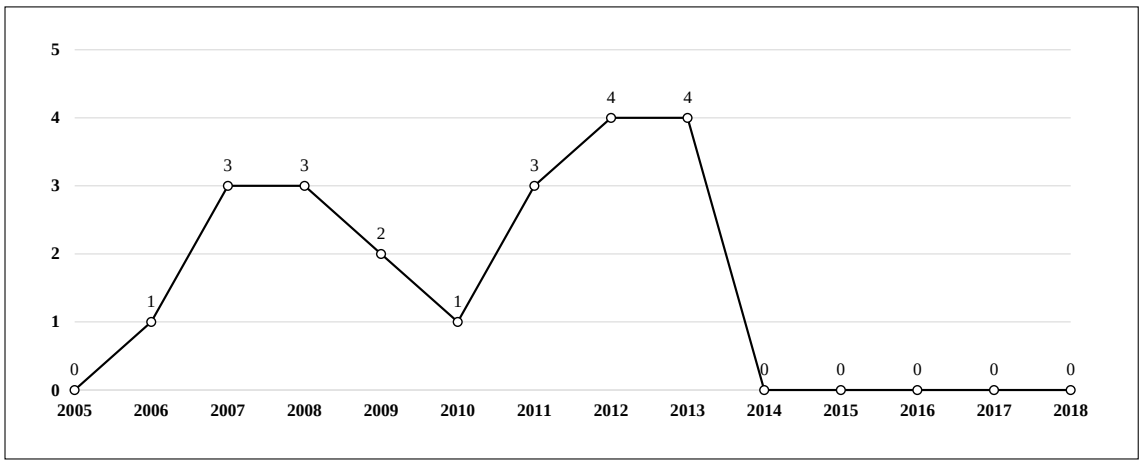


Figure 2.5: Trend of the publication of the primary studies during 2005-2018

Table 2.5: Detailed view of the primary studies

Title	Plan														Do			Check			Act		Overall
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
Chang, S Ernest	+	+									+												D
SREP	+	+						+	+							+							B
PrISM																		+	+	+		+	D
OntoWorks															+			+	+				D
SREPPLine	+	+	+				+	+	+							+							B
Boehmer, Wolfgang								+	+						+								D
ISSRM	+	+	+				+	+	+						+	+	+			+			P
AURUM	+	+						+	+							+	+						B
Valdevit, Thierry	+		+									+		+									D
Hensel, Veselina	+	+														+	+						D
HeRA	+	+		+																			D
SMP														+				+		+			D
5S2IS	+		+		+				+						+			+		+			B
I-SolFramework	+	+	+			+		+		+	+												B
SIEM															+	+	+						D
SCADA															+	+							D
Beckers, Kristian														+		+							D
"to be" environment								+								+	+						D
Asosheh, Abbass	+			+				+	+						+	+	+						B
PACTS	+	+		+	+			+						+	+	+							B
ISMS-CORAS	+	+	+	+				+	+					+	+	+	+						P

Note:
(D) Developing = Fulfil up to 4 criteria out of 22
(B) Basic = Fulfil between 5 to 9 criteria out of 22
(P) Proficient = Fulfil between 10 to 14 criteria out of 22
(A) Advanced = Fulfil more than 15 criteria out of 22

On the other hand, little to no evidence of some criteria detected such as Leadership (5), Policy (6), Resources (10), Competence (11), Awareness (12), Communication (13), Monitoring and measurement (18), Internal audit (19), Management review (20), Nonconformity and corrective action (21), and Continual improvement (22).

The results so far indicate that far too little attention paid to address all or most requirements of the standard. The number of studies in each category stands as below:

Developing = 12 Proficient = 2

Basic = 7 Advanced = 0

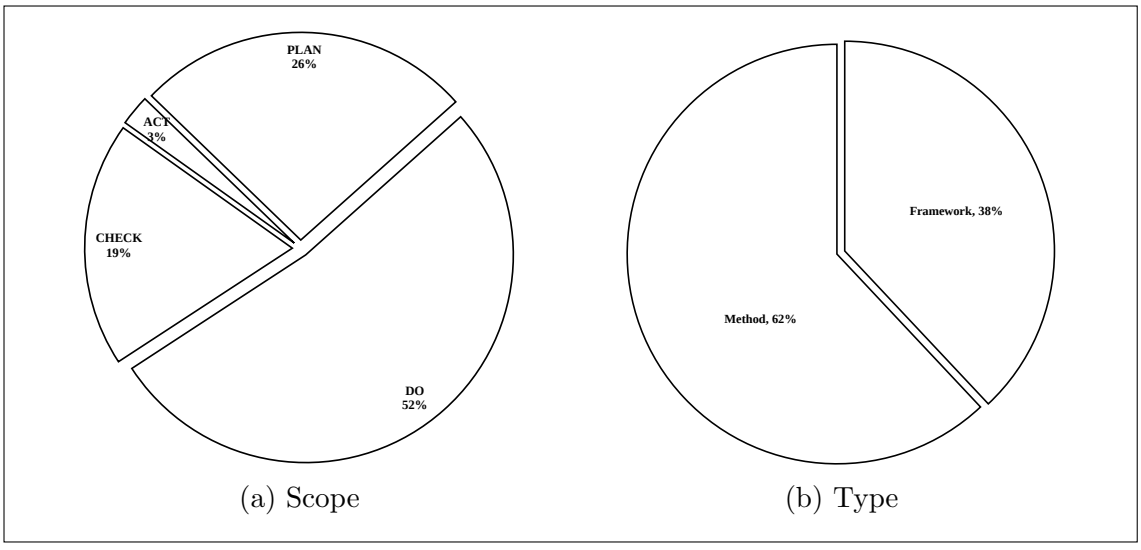
While some research produced in years in question, but only two studies attempted to investigate ISMS at the proficient level, i.e., fulfil between 10 to 14 criteria out of 22. No study found to reach the advanced level, meaning to support more than 15 criteria out of 22. The findings affirm that the majority (57%) of the selected studies are at the developing stage, i.e., only able to fulfil up to four (18%) requirements of the standard.

The average fulfilment rate of all the 21 studies is 23%, which is equivalent to five out of 22 requirements. Again, excluding any of the 22 requirements specified in Section 2.2.1 is not acceptable when an organisation claims conformity to the standard. Taken together, the current studies are incomplete and requires further expansion.

This interpretation contrasts with findings in Table 2.4, which provide detailed results about the scope of each study at the PDCA model.

Figure 2.6a illustrates that a considerable number of studies mostly fulfil the requirements of the Plan (26%) and Do (52%) stages, while, very few studies attempted to address Check (19%) and Act (3%) stages. The pie chart in Figure 2.6b shows the proportion of different types. It reveals that nearly two-thirds of studies were considered as Method, whereas only seven studies identified as Framework.

It is also worth noting that a distinct number of other articles, which dismissed during the selection process and not considered for this systemic literature review identified as Method. A note of caution is due here since not every study selected as part of our review claimed to meet every requirement of the standard and it could be argued that those study only focused on the indicated criteria or area of the standard; however, this suggests that there is a rudimentary gap in the knowledge.



(a) Scope (b) Type

Figure 2.6: Distribution of primary studies

2.3 Research Gaps and Challenges

The results presented in the investigation of the related work suggest specific gaps in the literature and highlight the need to address challenges in the area of ISMS. Together, five critical themes emerge from the studies discussed so far:

1. Holistic approach to capture the requirements of information security: information security encompasses a multitude of aspects categorised under confidentiality, integrity, and availability; however, an organisational structure includes many more aspects related to the operation and maintenance of the information security. All requirements of the standard need to be taken into account in order to holistically analyse security during the implementation of the ISMS. While the review of the related work identified a variety of attempts to address particular areas of the standard, support for the complete analysis of all areas are in short supply.
2. Support for analysis at multiple levels of abstraction: the representation of organisational processes in terms of strategies and policies should be accommodated in the context of information security management systems. The goals which an organisation aims to achieve by the execution of its processes can provide highly relevant input during the analysis and implementation phase. The propagation of security analysis through different levels of abstraction, from high-level organisational strategy to low-level services and implementation techniques, allows for a seamless transition from general security requirements to specific security configurations. It is, consequently, a unique approach for the design of secure business process and as such, it should be studied further by researchers of the area.
3. Ability to manage information security risk: comprehensive analysis of information security at the organisational level should facilitate all aspects of security requirements elicitation, and this includes the identification of threats, vulnerabilities and countermeasures. The inclusion of risk-related aspects further enhances the analysis of information security events, as they allow to effectively capture potential threats, evaluate their impact and propose mitigating configurations.
4. Decision support capabilities: the specification of security components should provide the capacity to support decision making during the implementation process of ISMS. The review of the literature suggests that future works could benefit from reasoning capability by establishing links between all aspects of security and implementation processes.

5. Structured and concise approach: the implementation of ISMS is a lengthy development which demands time and close participation from a range of stakeholders in organisations. A well-structured and defined process to guide the analysis and implementation of ISMS increase the efficiency and effectiveness of the implementation process. A less systematic approach such as poorly defined security-oriented notations could affect the use of future frameworks. Thus the introduce of intuitive and explicit security-related notations to cover all aspects of ISMS can enhance the effectiveness and usability of such frameworks and significantly reduce the effort required during the implementation stage. The focus of future attempts should support the creation of well-defined approaches to improve the implementation experience.

2.4 Research Baseline

This section describes the goal-oriented requirements engineering and its concepts, providing a baseline of the properties and common attributes. These explained through a domain-neutral perspective, where the goal is to provide a shared understanding of the underlying concepts in this research.

2.4.1 Goal-Oriented Requirements Engineering

GORE, as defined in Section 2.1.1, is a methodology to support actor and goal concepts from the early phase of system modelling. Throughout the following chapters, certain concepts from requirements engineering for representing general concepts and security engineering for representing security-oriented concepts introduced by the works of [26, 32, 45, 115].

Some of the main concepts that the thesis used as part of its development are including:

- Actor: actor can be a social agent, a position, or a role that represents an entity that has objective and strategic goals within a multi-agent system or organisational setting.
- Constraint: expresses a set of restrictions that do not allow specific actions from happening or avert particular objectives from being achieved by an actor or a system.
- Dependency: dependency between two actors expresses that one actor depends on the other to accomplish some security goal, fulfil a task, or deliver a resource. The former actor is called the depender, and the latter is called dependee. The type of dependency describes the nature of an object between dependee and depender referred to as dependum.

- Goal: goal represents a condition in the world that an actor would like to achieve. The concept of a (hard) goal differentiates from the concept of soft-goal. The soft-goal utilises to capture non-functional requirements of a system, soft-goal defines in methods that chosen in pursuing the hard-goal.
- Objective: security objectives represent a set of principles or rules that contribute to the achievement of the system's security.
- Security mechanism: represents standard security methods for helping towards the satisfaction of the security objectives. Some of these methods can prevent security attacks, whereas others are able only to detect security breaches.
- Threat: threat expresses situations that have the potential to create a loss or cause a problem that can put in danger the security features of the system.
- Vulnerability: vulnerability is a weakness or flaw in security context that exists from a resource, an actor and/or a goal.

2.4.2 Diagramming Platforms

The review of the literature and study of the related work indicates that the current platforms are not open to extensibility and all of the identified methods are limited to the features of the proposed platforms with limited options to extensibility, hence, this thesis required to identify a platform that provide the users with specific benefits of our modelling framework including:

- Extensive shape libraries
- Custom libraries
- Extensibility: Plugin, integrations
- Export format: jpg, png, svg, pdf
- Multiple pages: support connected and multi diagrams
- Arrangement: automatic layout
- Open-source
- Desktop support: Microsoft Windows, Mac
- Online: web-browser
- Free license

The above features enable the realisation of the proposed framework aim and objectives. Besides, the use of an existing platform avoids the unnecessary strain of time and fault finding of a new tool and allows the user of the framework to concentrate on the applicability of the framework rather than the excess efforts to use the framework itself.

The investigation of widely-used modelling and diagramming platforms which had to provide most or all of the above features shown and compared in Table 2.6.

Table 2.6: Diagramming platform comparison

Application	Cacoo	Draw.io	Gliffy Diagram	Lucidchart	Microsoft Visio	Omnigraffle	SmartDraw	Visual Paradigm
Shape libraries	+	+	+	+	+	+	+	+
Custom libraries	+	+	+	+	+	+	+	+
Extensibility	+	+	+	+	+	+	+	+
Export format	+	+	+	+	+	+	+	+
Multiple pages	+	+	+	+	+	+	+	+
Arrangement	+	+	+	+	+	+	+	+
Open-source		+						
Desktop (mac)		+				+		+
Desktop (windows)		+			+		+	+
Online (web)	+	+	+	+	+		+	+
Free license		+						

The features identified in each platform were available as of September 2019. Almost all platforms required paid subscription per user, device or one-off purchases; the community, limited or free trials were not recorded as a free license.

Draw.io supports all of the features required to meet this thesis's objectives, hence, used as recommended platforms to propose the concepts of the framework. Draw.io[10] [11] is an open-source technology stack for building diagramming applications, and a browser-based end-user diagramming application.

The concepts introduced in the following chapter and the workflow of the framework discussed in Chapter 4 make the use of the Draw.io version 11.2.5. All concepts introduced by the proposed framework were built-in as a standalone Plugin to enhance the experience of the framework users and to avoid any confusions in using the framework.

2.5 Summary

This chapter provided a review of the literature on the requirements of the ISMS as well as an overview of challenges and issues in the analysis and implementation of ISMS. This chapter aims to systematically investigate the approaches, which assist organisations analyse, implement, and conforms with the requirements of the stand-

[10]https://www.draw.io/

[11]Draw.io is a trading name of JGraph Ltd

ard. The review examined the methods thought to contribute to the requirements of the ISO/IEC 27001. The most prominent finding to emerge from this study is that substantial potential exists for academic researchers to investigate the ISMS under a holistic approach. The evidence from this review suggests that there is a gap in the current approaches to satisfy all requirements of the standard and comprehensive approaches recommended in advancing ISMS. The following chapter introduces a modelling language to capture and model the requirements of the standard coherently. Initially, it discusses the requirements for the proposed modelling language. Then, it describes the concepts used in the modelling language to address some of the gaps and challenges identified in this chapter.

Chapter 3

INFORMS Modelling Language

The previous chapter conclusively showed that prior studies have not been able to account for all aspects of the standard, and have been mostly exploratory without significant support for organisations to implement the standard. This chapter discusses INtegratable Framework for mOdelling Requirements of Management Systems (INFORMS) adopted to appropriately address the research questions and contain the requirements of the standard. This chapter aims to present a model-driven language to consider the current limitation of the literature as mentioned earlier and alleviate the gaps in knowledge. Next, it explains the overall description of the modelling language and a metamodel developed to support the language; it further explained by introducing the concepts of the language. Finally, it describes the proposed relationships between the concepts of the language.

3.1 Requirements of the Modelling Language

The developed modelling language aims to address the research gaps and limitations by making the following contributions:

- support for the elicitation and exercise of all aspects of the ISO/IEC 27001;
- alignment between high-level goals and operational level configurations;
- seamless transition between different abstraction of organisational layers supported via explicit mappings;
- support for stakeholders' inputs during decision-making at the operational level;
- adaptable approach to process model instantiation, where several designs can derive according to the specific situational needs;
- capacity to scale and adapt to future needs of an organisation;
- structured approach to guide the implementation process of ISMS;
- introduce concepts to identify, assess and evaluate information security risks;

– the language to include concise, simple and straightforward notation; and
– ability to capture the concepts of stakeholders conjunction with the requirements of the standard.

3.2 Modelling Language Overview

Organisations need to identify and implement the requirements of the ISMS to claim conformity with the standard. They need to be able to distinguish the requirements of the standard from other recommendations, where there is a certain freedom of choice. The implementation of the ISO/IEC 27001 is reasonably complex and includes a full multi-tier enterprise-scale components; managing these components and requirements is a challenging task that could result in misinterpretation or possibly forgotten when developing such a domain.

The standard itself is written using informal languages (natural language) and is notoriously obscured by the ambiguity and verbosity of the English language. While the natural language is flexible and allows communicating the standard to everyone, it is of little use when it comes to implementing the requirements of the standard. As described in Chapter 1, a correct understanding of the requirements of the standard is a challenging task for organisations aiming to implement the standard.

The findings of the literature indicate that there is no consensus on the interpretation of the standard and the completeness of the available analysis of the standard is incoherent; hence, this thesis has depended on the terms and definitions provided by the ISO/IEC 27000 as well as the provisions of the ISO/IEC Directives, Part 2, Principles and rules for the structure and drafting of ISO and IEC documents [1] to elicit the requirements of the standard.

Standards include many clauses and sub-clauses in the form of normative phrases. The structure of the interpretation followed using the aforementioned references and the functional analysis of the standard document, which indicates principle oriented characteristics that are evident in clauses of the standard. The construction for expressing the provisions include elemental components such as subject to action, normative phrase, action and object. It is plausible to invert the same methodology to elicit the requirements of the standard and contrive the proposed modelling language. The following is an example of how each clause analysed and interpreted using the same construction:

> ISO/IEC 27001:2013 - Clause 4.1:
> "The organization shall determine external and internal issues that are

[1] https://www.iso.org/sites/directives/current/part2/index.xhtml

relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system."

In the above clause, the subject is "organisation", the normative phrase is "shall", the action is "determine" and the object is "external and internal issues". The complete result of the analysis and interpretation of the standard was not permitted for publication in this thesis for copyright protection [2]. While the above clause provides a degree of precise construction without much verbosity, the object identified in the clause is still encoded. An actual interpretation of such clauses is mainly left to presumption and increased complexity when implementing the 52 mandatory clauses in the standard.

The INFORMS modelling language utilises requirements engineering techniques to enables the implementation and expression of the ISMS specifications. The objectives of the modelling language systemically analysed and aligned with the requirements of the standard as part of the development. One aim in the development of INFORMS is to avoid detail overload; the implementers of ISMS should be able to focus on implementing the requirements of the standard, rather how the components of the standard work.

The proposed language provides organisations with an aim-oriented approach to model ISMS by using specific and defined language and notations. It is constructed in structural and behavioural models using the Unified Modeling Language (UML) and notations represented in graphical symbols. UML is controlled by Object Management Group to ensures UML's transformability and interoperability across vendors. It is simply impractical to ask all the stakeholders of INFORMS to learn various implementation languages before they can interact with the language.

The INFORMS modelling language underpinned by a model known as the INFORMS meta-model to define the relationships between all the components of the standard. It ensures the language is used and applied consistently. Also, models that created from the language using the meta-model may homogeneously exchange inputs and outputs amongst other models within the language.

The meta-model illustrated in UML notations is shown in Figure 3.1. It provides a simplification of the ISMS to facilitates the structure of the standard to be understood, evaluated, and criticised. It specifies the data exchange format for the architecture of the INFORMS framework. The semantics of the modelling language captured in the meta-model, backed by 10 concepts and a family of graphical notations described in the following section.

[2]The author sought to receive the necessary permissions for publishing and distributing the results of the analysis from the copyright holder of the standard document, however, it was not granted.

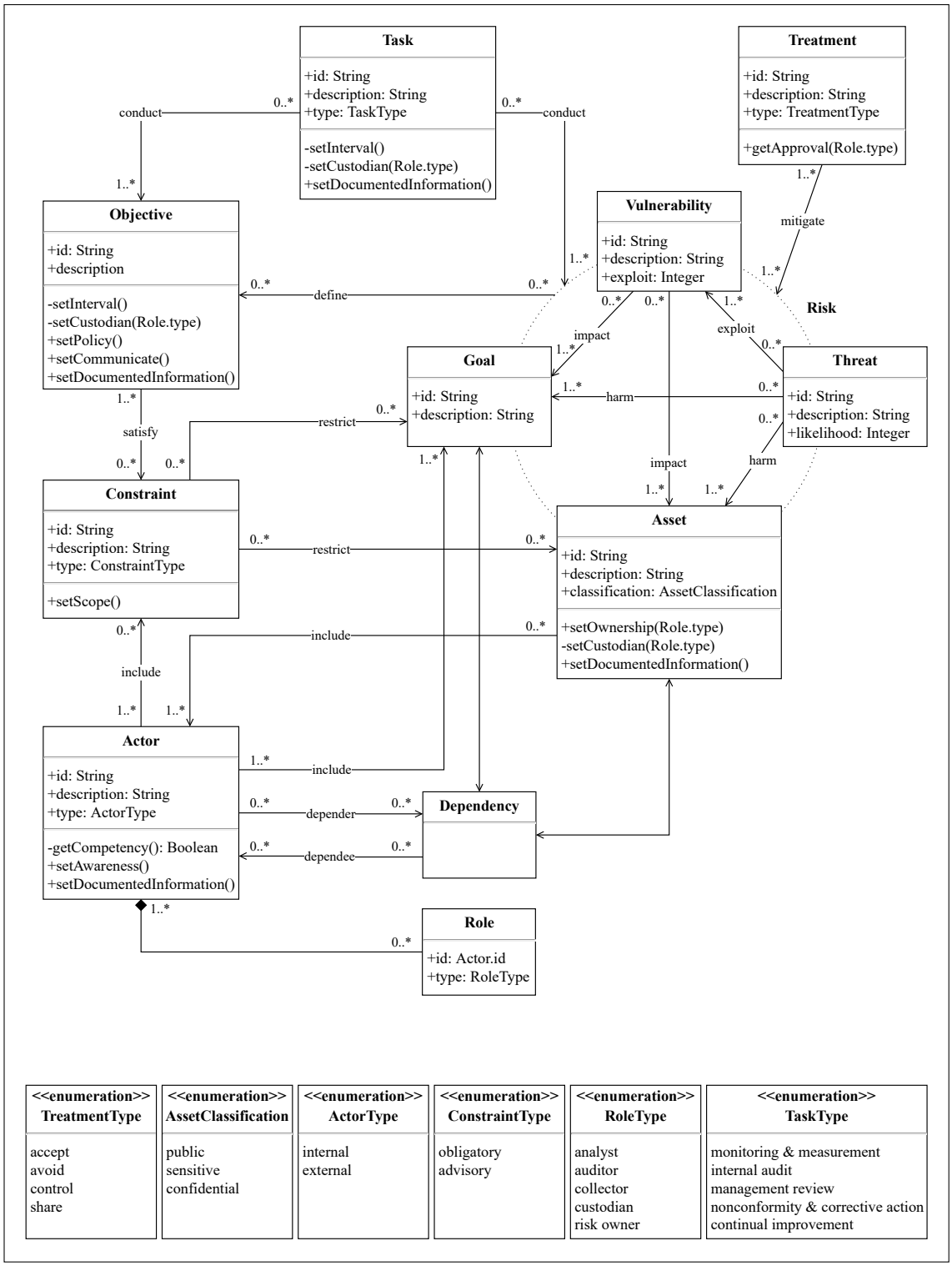


Figure 3.1: INFORMS meta-model

The operations included in the classes of the INFORMS modelling language described within the definition of each relevant view in the next chapter. The attributes or properties shown in one class may be shared and used similarly in more than one class, e.g., ID, Description. The naming conventions used for the modelling language are as follow:

– Class names start with upper-case.
– Attributes and Operations names are lower camel case.
– Attributes type names are upper camel case.
– Association names start with lower-case.

3.3 Concepts

This section defines each class of the meta-model along with their conceptual meaning. The concepts are discussed from the structural perspective, while their dynamic characteristics are discussed in the INFORMS framework in Chapter 4.

3.3.1 Actor

An actor represents a person or entity that has a strategic goal(s) within its organisational setting relevant to the scope of the ISMS. An actor could have a direct or indirect effect, be affected by, or perceive themselves to be affected by a decision or activity relevant to information security. An actor does not necessarily have to be an actual person or entity, and it could include a process.

An actor could refer to as user or stakeholder, however, the definition in the INFORMS modelling language captures the characteristics and capacity of an actor within the scope of the ISMS. An actor could be both an independent person(s) like a client, an employee, a group of community, or interested parties like shareholders, as well as an entity like a national authority such as Information Commissioner's Office (ICO) or GDPR. The graphical notation for an actor is presented in Figure 3.2a as a pink circle.

The types of actors categorised as an *internal* and *external actor*. The former type refers to the internal context of the organisation who benefits from the success of the ISMS, such as shareholders and owners of an organisation with a commercial interest in the success of the ISMS or an employee by contributing to the effectiveness of the ISMS. External actor refers to the external context of the organisation who expects a certain level of service or due care from the organisation such as clients or local and international regulatory entities.

The number of actors in an ISMS depends on the nature of the organisation, and the scope of the ISMS, e.g., an accounting firm with global offices could have a more significant number of actors compares to a local manufacturer; the depth and inclusion of actors for each organisation are different. Actor's class as illustrated in Figure 3.2b, include three properties listed below.

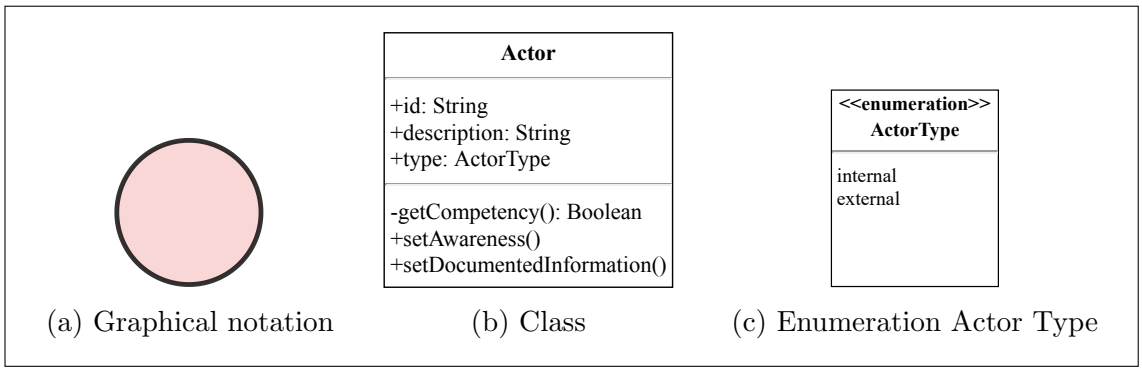
– ID: indicates an exclusive presentation of an actor placed in the centre of an actor's graphical notation. It helps to effectively manage the scalability

of actors in more extensive settings and interoperability of the concept in the INFORMS modelling language. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letters AC accompanied by a unique digit, e.g., AC1, AC2, AC3.

- Description: presents the description of an actor's title within the organisation, e.g., personnel, client. This attribute is defined as a String data type and tagged by public visibility.
- Type: describes the type of an actor and has an enumeration named identifier of Actor Type, which includes two enumeration literals of internal and external as shown in Figure 3.2c. This attribute tagged by public visibility.

Actor's class provides three operations to illustrates specific behavioural processes of the framework, including:

- Get Competency: refers to the competency level of an actor doing work under its control that affects its information security performances. The operation corresponds to the Actors Description View described in Section 4.3.1 and tagged by private visibility.
- Set Awareness: provides inputs to the Awareness View described in Section 4.2.4 and tagged by public visibility.
- Set Documented Information: provides inputs to the Documented Information View described in Section 4.2.6 and tagged by public visibility.



(a) Graphical notation (b) Class (c) Enumeration Actor Type

Figure 3.2: Actor

3.3.2 Asset

An asset is anything that has value for the organisation relevant to information security. An asset does not necessarily refer to the monitory value of an item and it could include tangible and intangible assets. An accurate recognition of an asset's criticality ensures that it receives an appropriate level of protection relevant to its importance to the ISMS. Some of the key assets are the information in rest or in

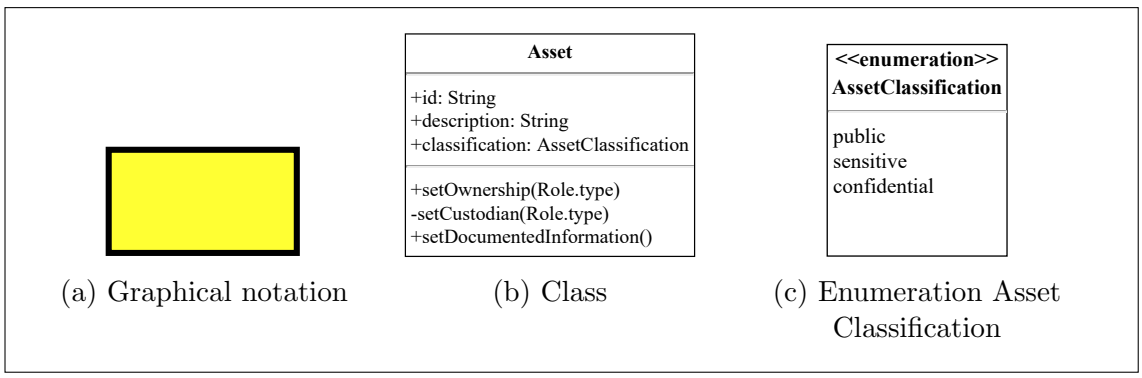
transit that must be protected and taken into consideration when implementing an ISMS.

The graphical notation for an asset is shown in Figure 3.3a as a yellow rectangle. Asset's class as illustrated in Figure 3.3b, include three properties listed below.

- ID: indicates an exclusive presentation of an asset placed in the centre of an asset's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letter *A* accompanied by a unique digit, e.g., A1, A2, A3.
- Description: presents the description of an asset as identified in the inventory of assets, e.g., printer, Microsoft Windows, client's personal information. This attribute is defined as a String data type and tagged by public visibility.
- Classification: indicates an asset's sensitivity to the organisation. Information classification specifies how personnel to handle specific information; determining the classification of an asset should be in accordance with the information classification scheme adopted by the organisation. The attribute has an enumeration named identifier of Asset Classification, which includes three enumeration literals as shown in Figure 3.3c.

Asset's class provides three operations to illustrates certain behavioural processes of the framework, including:

- Set Ownership: provides an input to the risk ownership responsibility for an asset. The type of input corresponds to the risk owner Role Type discussed in Section 3.3.6 and tagged by public visibility.
- Set Custodian: provides an input to the custodian responsibility for an asset. The type of input corresponds to the custodian Role Type discussed in Section 3.3.6 and tagged by private visibility.
- Set Documented Information: provides inputs to the Documented Information View described in Section 4.2.6 and tagged by public visibility.



(a) Graphical notation (b) Class (c) Enumeration Asset Classification

Figure 3.3: Asset

3.3.3 Constraint

A constraint is a stipulation of restrictions and boundaries on assets and goals introduced by an actor. An organisation should identify the requirements, issues and expectations of actors as part of the ISMS. A constraint does not permit a specific action or set of actions to be deployed or limit particular objectives from being achieved against the expectation of the actor(s).

An organisation needs to have an in-depth consideration of each actor's constraint; it may need to seek legal or expert advice on meeting particular constraints to ensure it correctly satisfies the expectations of its actors.

Not all constraints from actors are equally important in their application and organisations must prioritise the order of fulfilling constraints to avoid conflict. Also, this allows effective and efficient use of resources and strategic alignment of the organisation's security policy to satisfy most concerning constraints than trivial ones. In considering the importance of prioritisation of constraints, INFORMS proposes two types of constraint:

Obligatory is non-negotiable and often imposed by external actors. The organisation has no control over their exclusion or the execution of them, e.g., a regulatory requirement or contract by a government authority. The graphical notation for an obligatory constraint is shown in Figure 3.4a as a purple octagon with a divider in the top and labelled with the word *obligatory*.

Advisory is negotiable and can be introduced by any types of actors. The organisation has execution capability to alter the provision or limit the implementation of the constraint. The graphical notation for an advisory constraint is shown in Figure 3.4b as a purple octagon with a divider in the top and labelled with the word *advisory*.

For example, an IT manager of an organisation based in Germany develops an information retention policy that limits the organisation to "retain the clients' information for up to eight years". In contrast, EU GDPR expects that "personal data must not be kept for longer than is necessary", and failure to adhere to such regulation can result in legal enforcement and administrative fines [116].

In this scenario, the constraint introduced by the EU GDPR (external actor) supersedes the constraint initiated by the IT manager (internal actor); the implementation of the EU GDPR is mandatory and the retention policy developed by the IT manager could be revised. The constraint introduced by the external actor is obligatory and the constraint introduced by the internal actor is advisory. However, the advisory constraint conflicts with the obligatory constraint and should not be

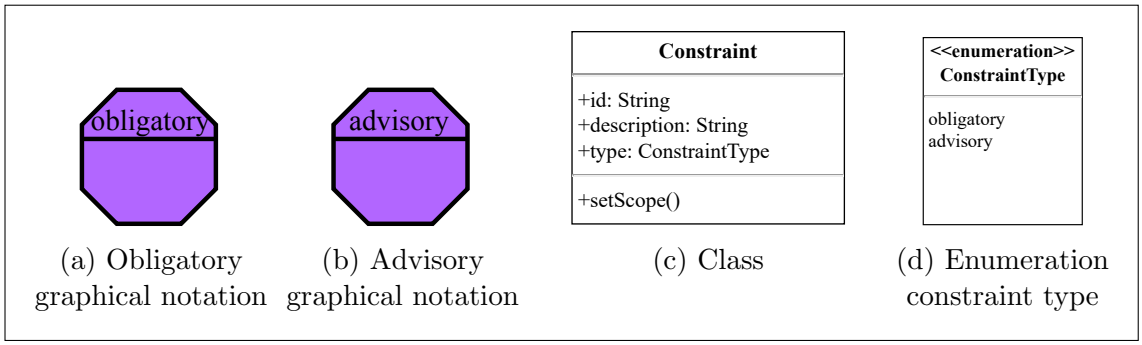
satisfied unless the retention policy aimed at data subjects residing outside of the European Union.

Constraint's class as illustrated in Figure 3.4c, include three properties listed below.

- ID: indicates an exclusive presentation of a constraint placed in the centre of a constraint's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letter *C* accompanied by a unique digit, e.g., C1, C2, C3.
- Description: presents the description of a constraint propounded by an actor for consideration, e.g., as part of a privacy agreement of a contract with an external actor, the actor may request that all personal information must be transmitted using a secure channel. This attribute is defined as a String data type and tagged by public visibility.
- Type: describes the type of a constraint and has an enumeration named identifier of Constraint Type, which includes two enumeration literals of obligatory and advisory as shown in Figure 3.4d. This attribute tagged by public visibility.

Constraint's class provides one operation to illustrates specific behavioural processes of the framework, including:

- Set Scope: provides inputs to the Scope View described in Section 4.2.1 and tagged by public visibility.



(a) Obligatory graphical notation (b) Advisory graphical notation (c) Class (d) Enumeration constraint type

Figure 3.4: Constraint

3.3.4 Goal

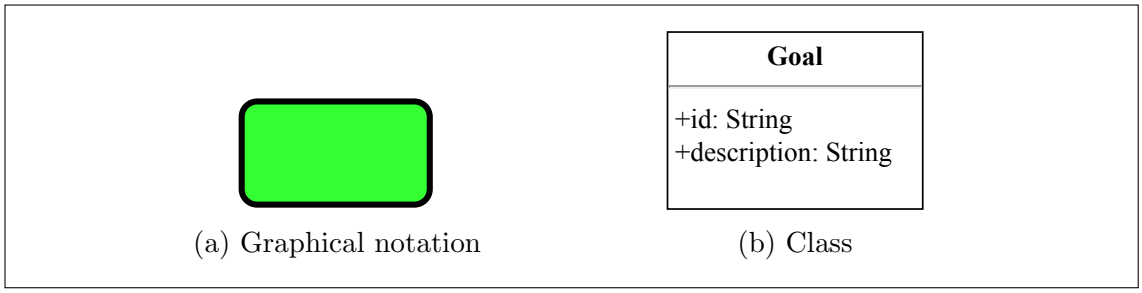
An actor has goals that are strategically critical for the continuity of the organisation, i.e., Goal refers to an actor's strategic interests in the organisation. It is part of the actor's identity to have his/her goals accomplished while it is the responsibility of the organisation to support the achievement and delivery of the actor's goals.

Goals establish to describe the intended future state; they identify and provide

direction to activities and orient those activities towards the desired effect. Goals can be expressed as enterprise goals, high-level strategic goals that apply to the entire organisation or as more specific operational goals that define desired outcomes of a work process.

Actors' goals have a pivotal role in the effectiveness of the information security management system. Goals are planned activities to be achieved and could lead to success or failure of the information security management system if not identified or addressed appropriately by the organisation. The graphical notation for a goal is shown in Figure 3.5a as a light green rounded rectangle. Goal's class as illustrated in Figure 3.5b, include two properties listed below.

- ID: indicates an exclusive presentation of a goal placed in the centre of a goal's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letter *G* accompanied by a unique digit, e.g., G1, G2, G3.
- Description: presents the description of a goal delivers to or by the organisation propounded by an actor for consideration, e.g., an IT manager would like to implement cloud storage for better accessibility of remote personnel. This attribute is defined as a String data type and tagged by public visibility.



(a) Graphical notation (b) Class

Figure 3.5: Goal

3.3.5 Objective

Information security objective defines the strategic and organisation-wide information security aims to be achieved; security objectives can be defined in terms of the organisation's overall mission. The security objectives are similarly defined and influenced by actors' goals, assets, constraints, information security risks. Security objectives do not have priorities, unlike constraints; they are mutually exclusive.

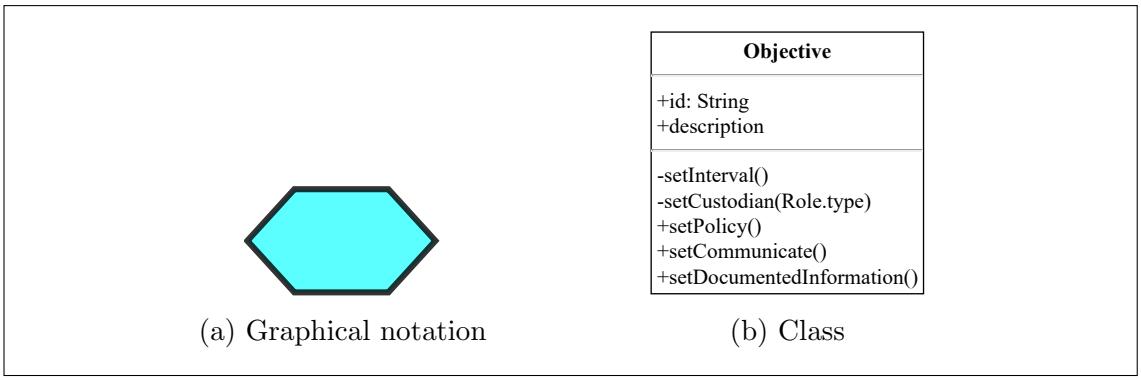
The overall objective is to implement a range of initiatives that collectively achieve all of the security objectives; one or more initiatives fulfil each security objective. An initiative is the implementation of an operational plan that achieves part or all of the security objectives. The graphical notation for an objective is

shown in Figure 3.6a as a light blue hexagon. Objective's class as illustrated in Figure 3.6b, include two properties listed below.

- ID: indicates an exclusive presentation of an objective placed in the centre of an objective's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letter *O* accompanied by a unique digit, e.g., O1, O2, O3.
- Description: description of an information security objective defined by the organisation, e.g., "To maintain the confidentiality and integrity of personal information at all time". This attribute is defined as a String data type and tagged by public visibility.

Objective's class provides four operations to illustrates certain behavioural processes of the framework, including:

- Set Interval: provides value for the completion period of an objective. It corresponds to the Objectives Specification View discussed in Section 4.5.2 and tagged by private visibility.
- Set Custodian: provides an input to the custodian responsible for an objective. The type of input corresponds to the custodian Role Type discussed in Section 3.3.6 and tagged by private visibility.
- Set Policy: provides inputs to the Policy View described in Section 4.2.3 and tagged by public visibility.
- Set Communication: provides inputs to the Communication View described in Section 4.2.5 and tagged by public visibility.
- Set Documented Information: provides inputs to the Documented Information View described in Section 4.2.6 and tagged by public visibility.



(a) Graphical notation (b) Class

Figure 3.6: Objective

3.3.6 Role

A role is a fundamental characteristic of an actor with a capacity to be assigned a particular responsibility to accomplish specific requirements of ISMS. Organisations

may assign more than one role type to an actor in the ISMS as long as the roles do not conflict with the overall interest of the actor in the organisation. For example, an IT manager is not a suitable candidate to audit the IT department, while the same manager can act as auditor for other departments.

INFORMS offers five types of roles to use at the required steps of the framework, are listed below.

Analyst is responsible for analysing data in measurement-related requirements of the ISMS. The graphical notation for the analyst is shown in Figure 3.7a as a pink circle with a divider in the top and labelled with the word *analyst*.

Auditor is responsible for conducting internal audit and evaluating the effectiveness of the ISMS. The graphical notation for the auditor is shown in Figure 3.7b as a pink circle with a divider in the top and labelled with the word *auditor*.

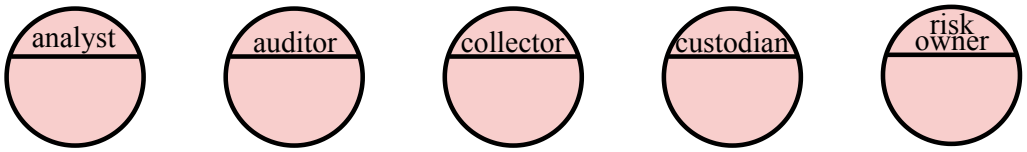
Collector is responsible for collecting and recording data in measurement-related requirements of the ISMS. The graphical notation for the collector is shown in Figure 3.7c as a pink circle with a divider in the top and labelled with the word *collector*.

Custodian is responsible for maintaining and providing a duty of care towards an object in the ISMS, e.g., an IT manager could assign provision and enforcement of access to the server room to a technician as a full-time task, who acts as a custodian to maintain the server room. The graphical notation for the custodian is shown in Figure 3.7d as a pink circle with a divider in the top and labelled with the word *custodian*.

Risk owner is an actor or entity accountable to oversee and administer risk-related decisions, e.g., an IT manager of an organisation is responsible for the server room and is accountable for unauthorised access to the facility. While the IT manager (risk owner) may not be responsible for maintaining access to the server room and may assign this duty to another actor, the IT manager is accountable in the occurrence of a risk. The graphical notation for a risk owner is shown in Figure 3.7e as a pink circle with a divider in the top and labelled with the word *risk owner*.

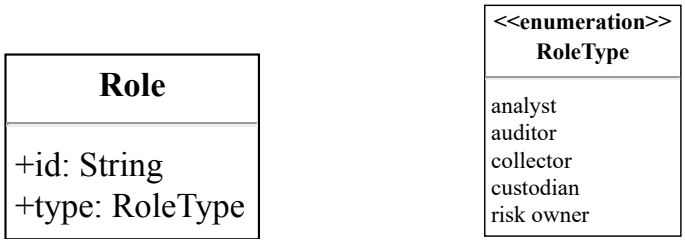
Role's class as illustrated in Figure 3.8a, include two properties listed below.

- ID: refers to the ID of an actor allotted in the actor's class and placed in the centre of the relevant role's graphical notation. Any changes to an actor's ID reverberate in the role's ID.
- Type: describes the type of a role and has an enumeration named identifier of Role Type. It includes five enumeration literals of analyst, auditor, collector, custodian and risk owner as shown in Figure 3.8b. This attribute tagged by public visibility.



(a) Analyst (b) Auditor (c) Collector (d) Custodian (e) Risk owner

Figure 3.7: Role graphical notation



(a) Class (b) Enumeration role type

Figure 3.8: Role

3.3.7 Task

Almost all the concepts introduced by the INFORM modelling language functioned to fulfil the requirements of the ISMS, on the other hand, task provides the means to verify the fulfilment of the requirements as well as the overall validation of the ISMS. Task expresses a set of inclusive methods to asses and maintain the performance of ISMS.

The INFORMS modelling language proposes Task, to evaluate the performance of the ISMS. It incorporates a set of methods to identify opportunities to enhance the pertinence of the ISMS implementation as expected by the standard. It offers five types of task to manage specific requirements of the standard, are listed below.

Monitoring and measurement assists the organisation in understanding the status of an information system or processes by determining a value, e.g., treatment or threat threshold. The graphical notation for the monitoring and measurement is shown in Figure 3.9a as a grey square labelled with the word *task* and a divider in the top and letters *MM* placed in the centre.

Internal audit provides detailed information on the conformity of the organisation to the requirements of the ISMS and the organisation. The graphical notation for the internal audit is shown in Figure 3.9b as a grey square labelled with the word *task* and a divider in the top and letters *IA* placed in the centre.

Management review refers to the top management review of the ISMS suitability and effectiveness to ensure its alignment with the information security objectives. The graphical notation for the management review is shown in Figure 3.9c as a grey square labelled with the word *task* and a divider in the top and letters *MR* placed in the centre.

Nonconformity and corrective action identifies the non-fulfilment of a requirement of the ISMS. The graphical notation for the nonconformity and corrective action is shown in Figure 3.9d as a grey square labelled with the word *task* and a divider in the top and letters *NC* placed in the centre.

Continual improvement identifies the opportunities to improve the suitability, adequacy and effectiveness of the ISMS. The graphical notation for the continual improvement is shown in Figure 3.9e as a grey square labelled with the word *task* and a divider in the top and letters *CI* placed in the centre.

Task's class as illustrated in Figure 3.10a, include three properties listed below.

- ID: indicates an exclusive presentation of a task placed in the centre of a task's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letters of the task types described above accompanied by a unique digit, e.g., MM1, IA1, MR1, NC1, CI1.
- Description: a reflective description of a task type, e.g., An organisation wish to monitor and measure the physical access to the organisation by intruders. This attribute is defined as a String data type and tagged by public visibility.
- Type: describes the type of a task and has an enumeration named identifier of Task Type. It includes five enumeration literals as shown in Figure 3.10b. This attribute tagged by public visibility.

Task's class provides three operations to illustrates certain behavioural processes of the framework, including:

- Set Interval: provides value for the completion period of a task. It corresponds to each relevant view in the Standard Viewpoint discussed in Section 4.6 and tagged by private visibility.
- Set Custodian: provides an input to the custodian responsible for a task type. The type of input corresponds to the custodian Role Type discussed in Section 3.3.6 and tagged by private visibility.
- Set Documented Information: provides inputs to the Documented Information View described in Section 4.2.6 and tagged by public visibility.

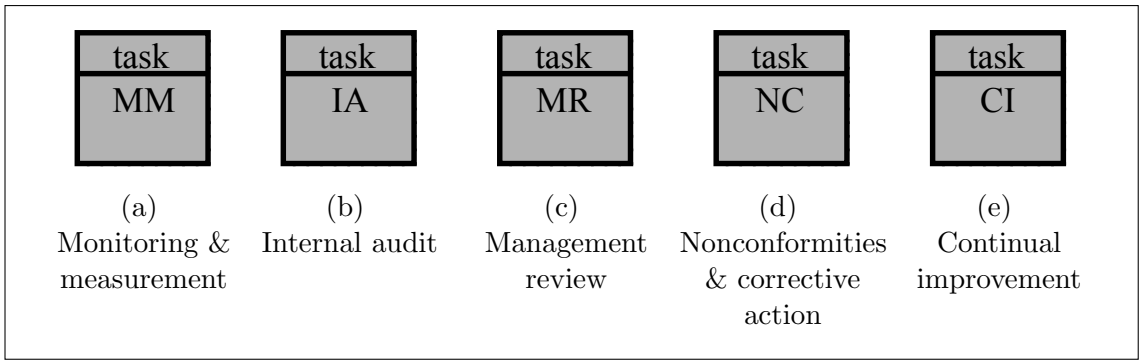
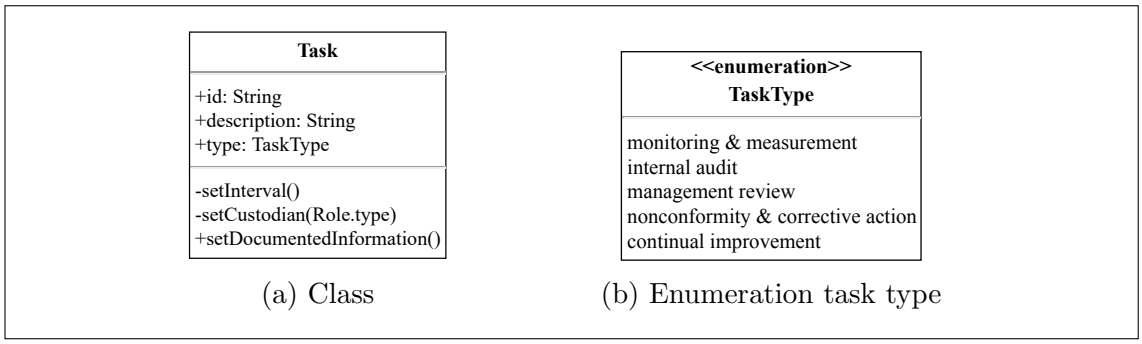


Figure 3.9: Task graphical notation



(a) Class (b) Enumeration task type

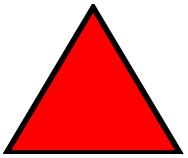
Figure 3.10: Task

3.3.8 Threat

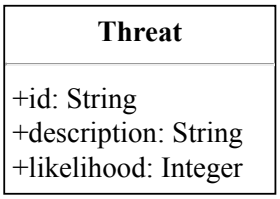
A threat describes the potential cause of an unwanted incident, which could affect the information assets or goals of the organisation. The cause of a threat could be accidental or deliberate from a natural or human origin, placed within or from outside the organisation.

The likelihood is the probability of something to happen, the measurement or estimate of a cause of an event to provide a complete result of the risk while assessing the threat. The graphical notation for a threat is shown in Figure 3.11a as a red triangle. Threat's class as illustrated in Figure 3.11b, include three properties listed below.

- ID: indicates an exclusive presentation of a threat placed in the centre of a threat's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letter T accompanied by a unique digit, e.g., T1, T2, T3.
- Description: presents the description of a threat, e.g., flood or remote spying. This attribute is defined as a String data type and tagged by public visibility.
- Likelihood: indicates the severity of the cause of a threat. This attribute is defined as an Integer data type and tagged by public visibility.



(a) Graphical notation



(b) Class

Figure 3.11: Threat

3.3.9 Treatment

A treatment is the overall course of action to modify risk. The action involves selecting a treatment type, identifying appropriate controls to implement the treatment, developing a treatment plan and obtaining approval of the treatment plan from the risk owner. A treatment decision made for each risk should be treated according to one or more treatment type included below. The graphical notation for the treatment is depicted in Figure 3.12a as a green diamond triangle.

Accept to knowingly and objectively accept a risk; providing the level of risk satisfies the risk acceptance criteria. No need to implement additional treatment control and the risk can retain.

Avoid to avoid an activity or condition that increase the chance of a risk. A decision to avoid risk entirely by withdrawing from the root cause of the risk or changing the conditions under which the risk scenario operates. Also, the avoid treatment type is considered when the level of risk is high, or the costs of other treatment options exceed the benefits. For example, risks caused by natural sources could be avoided by physically moving the information processing facilities to a place where the risk does not exist or is under control.

Control to manage the level of risk by introducing, removing or altering controls so that the residual risk can reassess as being acceptable. Appropriate and justified controls should be selected to meet the risk acceptance criteria. Treatment controls could categorise by their type of protection, such as correction, elimination, prevention, deterrence, detection, recovery, monitoring, and awareness.

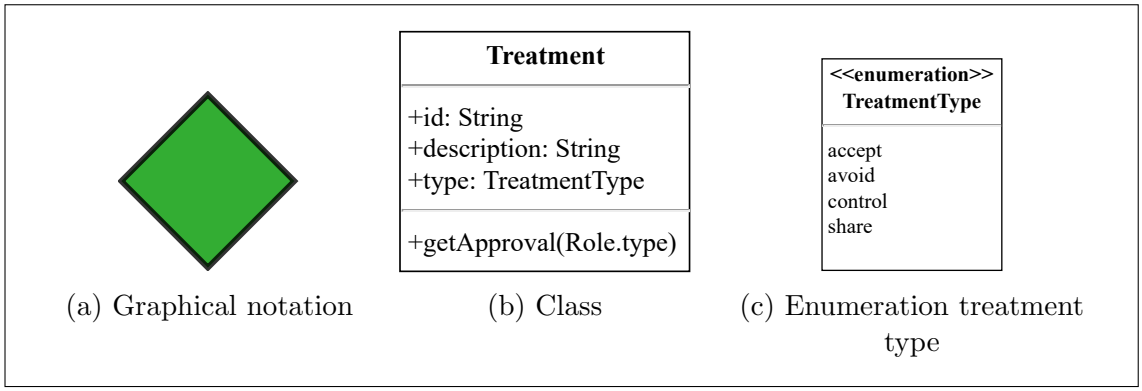
Share to share risk with another party that can most effectively manage a particular risk depending on risk evaluation criteria. Sharing a risk can create new risks or modify existing ones; therefore, additional risk treatment may be necessary.

Treatment's class as illustrated in Figure 3.12b, include three properties listed below.

– ID: indicates an exclusive presentation of a treatment plan placed in the centre of a treatment's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letters *TC* accompanied by a unique digit, e.g., TC1, TC2, TC3.
– Description: presents the description of a treatment plan, e.g., secure disposal of media. This attribute is defined as a String data type and tagged by public visibility.
– Type: describes a type of treatment and has an enumeration named identifier of Treatment Type. It includes four enumeration literals as shown in Figure 3.12c. This attribute tagged by public visibility.

Treatment's class provides one operation to illustrates certain behavioural processes of the framework, including:

– Get Approval: provides input from an asset's risk owner as established in the Asset class. The type of input corresponds to the Asset Management View in Section 4.3.3 and tagged by public visibility.



(a) Graphical notation (b) Class (c) Enumeration treatment type

Figure 3.12: Treatment

3.3.10 Vulnerability

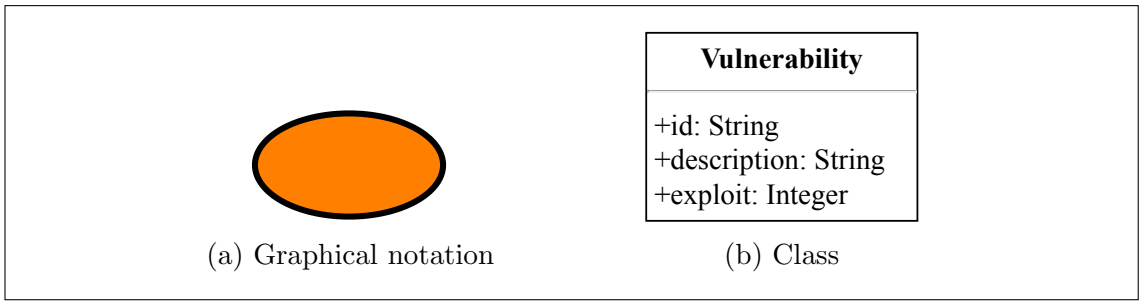
A vulnerability is a weakness of an asset or goal which could be exploited by one or more threats. The presence of vulnerability does not cause harm by itself if a threat does not trigger it. Each asset or goal could be harmed by a vulnerability if there is a corresponding threat.

The ease to exploit a vulnerability is a measuring attribute to describe the scale of a frequency that an exploit to be detected; the higher the frequency, the greater the harm to assets or goals. The graphical notation for a vulnerability is shown in Figure 3.13a as an orange ellipse. Vulnerability's class as illustrated in Figure 3.13b, include three properties listed below.

– ID: indicates an exclusive presentation of a vulnerability placed in the centre

of a vulnerability's graphical notation. This attribute is a String data type and tagged by public visibility. It follows a naming convention initiates with the letter *V* accompanied by a unique digit, e.g., V1, V2, V3.

– Description: presents the description of the vulnerability, e.g., insufficient media encryption. This attribute is defined as a String data type and tagged by public visibility.
– Exploit: describes the severity of potential harm to assets or goals subject to a successful attack. This attribute is defined as an Integer data type and tagged by public visibility.



(a) Graphical notation (b) Class

Figure 3.13: Vulnerability

3.4 Relationships

Relationships have cardinalities or other rules added to indicate how many of one instance of a class relates to an instance of another class and the necessity of such relations. The following sections outline the ten relationships proposed by the INFORMS modelling language, linking together concepts and define the relationships by building upon the meta-model introduced in Section 3.2.

3.4.1 Conduct

The Conduct association highlights the relationship between a Task class and an Objective class or a Task class and an information security risk. Figure 3.14a depicts a unidirectional *conduct* association drew as a solid line with an open arrowhead pointing to an Objective class. A similar demonstration is shown in Figure 3.14b for associating a Task to an information security risk.

The cardinality of a Task in relation to an objective or risk is [1..*], indicative of task conduct at least one objective or risk. A multiplicity association between an Objective or risk is [0..*] since they could have no corresponding task or conduct by many tasks.

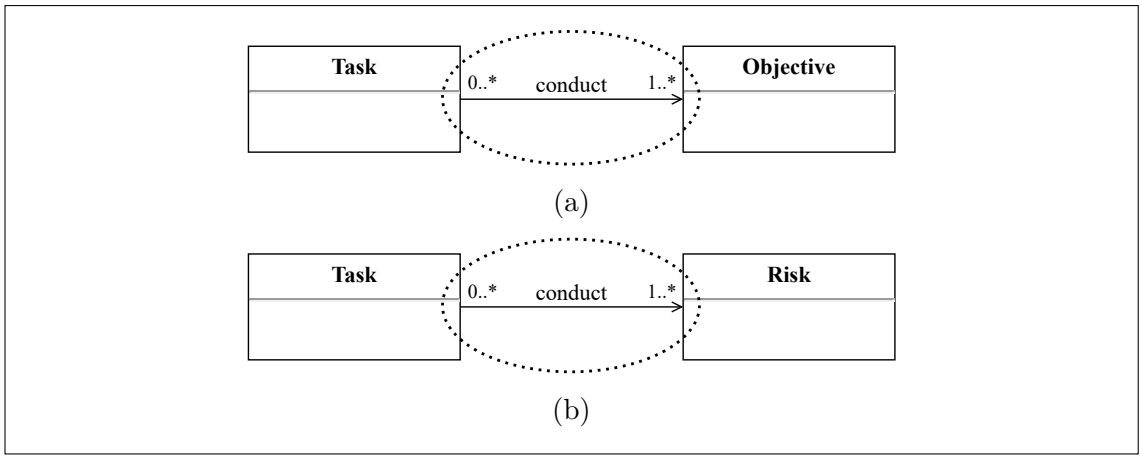


Figure 3.14: Conduct relationship

3.4.2 Define

The Define association describes the relationship between an information security risk and an Objective class. Figure 3.15 shows a unidirectional *define* relationship drew as a solid line with an open arrowhead pointing to an Objective class from an information security risk.

The cardinality of an information security risk to an Objective is [0..*], which translates to risk may contribute to the definition of none or many objectives. Similarly, a multiplicity association from an Objective to risk is [0..*] since it could have no corresponding risk or define by more than one risk.

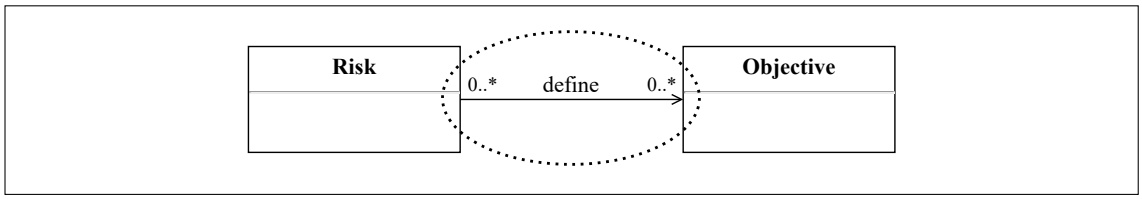


Figure 3.15: Define relationship

3.4.3 Dependency

Dependency relationship between two actors represents that one actor depends on the other to attain some goal or deliver an asset. The depending actor is called the *depender* and the goal/asset who is depended upon is called the *dependee*.

The dependency between actor (depender) and goal/asset (dependee) expresses that an actor depends on a goal or an asset to accomplish its purpose or access to an asset. The dependee is required to perform a given activity. The type of dependency describes the nature of an object or agreement between dependee and depender referred to as *dependum*.

By depending on the dependee for the dependum, the depender can attain goals that it is difficult or not possible to accomplish on its own, on the contrary, the depender becomes vulnerable since if the dependee fails to provide the dependum, the depender is affected in its aim to fulfil the goal [117, 115]. Asset dependencies require the dependee to provide an asset to the depender. Figure 3.16 presents the Dependency relationship graphical notation.

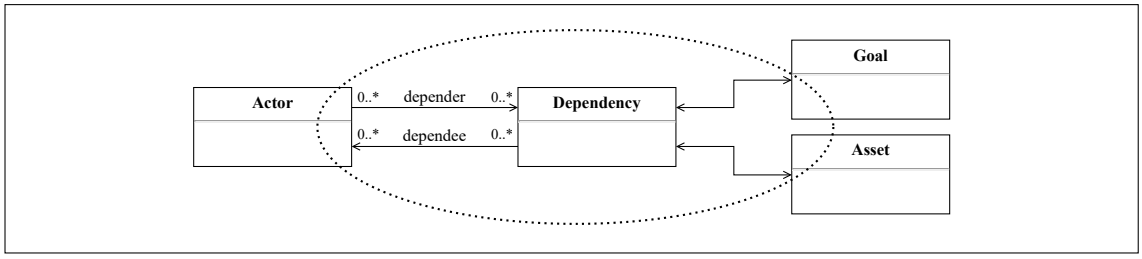


Figure 3.16: Dependency relationship

3.4.4 Exploit

The Exploit association describes the relationship between a Threat class and a Vulnerability class. Figure 3.17 shows a unidirectional *exploit* relationship drew as a solid line with an open arrowhead pointing to a Vulnerability from a corresponding Threat.

The multiplicity of a Threat to Vulnerability is [1..*], which indicates a threat may exploit one or many vulnerabilities. On the other hand, a multiplicity association from a Vulnerability to a Threat is [0..*], which shows vulnerability with no threat is not exploitable, or vulnerability may exploit with many threats.

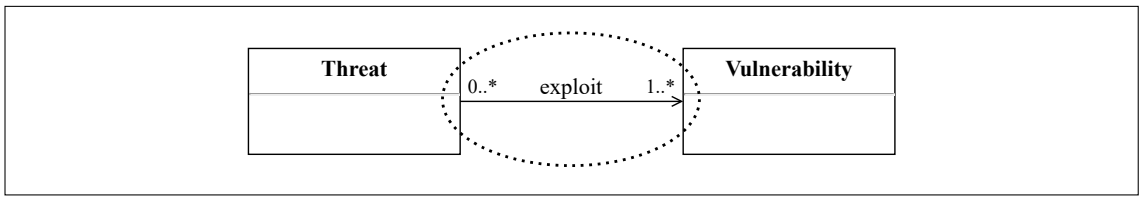


Figure 3.17: Exploit relationship

3.4.5 Harm

The Harm association describes the relationship between a Threat and its effect on Goal and/or Asset. Figure 3.18a depicts a unidirectional *harm* association drew as a solid line with an open arrowhead pointing to a Goal class. A similar demonstration is shown in Figure 3.18b for associating a Threat to an Asset.

The cardinality of a Threat class in relation to a Goal or Asset class is [1..*], indicative of a threat could harm at least one goal or asset. A multiplicity association

between a Goal or Asset to a Threat is [0..*] since they could have no corresponding threat or as many threat as applicable.

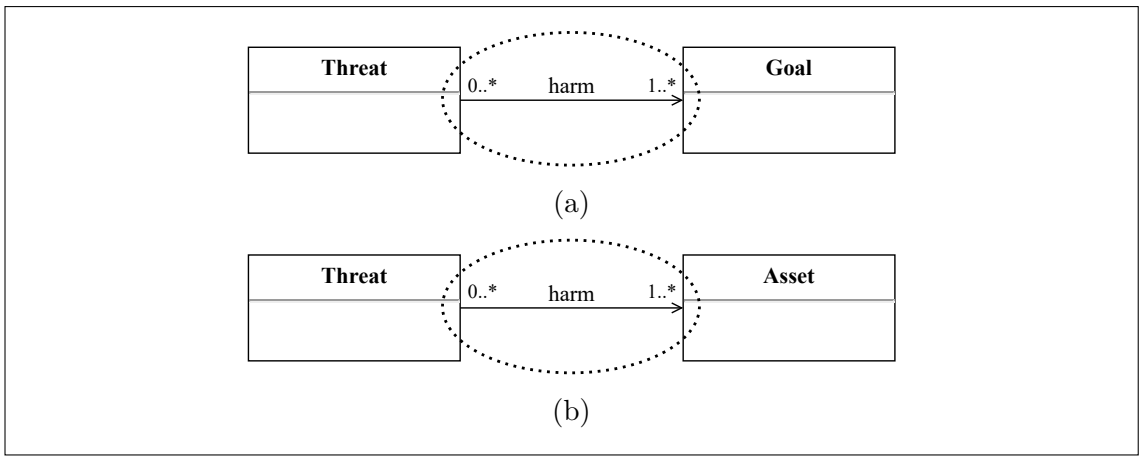


Figure 3.18: Harm relationship

3.4.6 Impact

The Impact association describes the relationship between Vulnerability and its impact on an Asset and/or Goal. Figure 3.19a depicts a unidirectional *impact* association drew as a solid line with an open arrowhead pointing to a Goal class. A similar demonstration is shown in Figure 3.19b for associating Vulnerability to an Asset.

The impact cardinality of a Vulnerability class in relation to a Goal or Asset class is [1..*], indicative of vulnerability could impact at least one goal or asset. A multiplicity association between a Goal or Asset to a Vulnerability is [0..*] since they could have no corresponding vulnerability or impacted by many vulnerabilities.

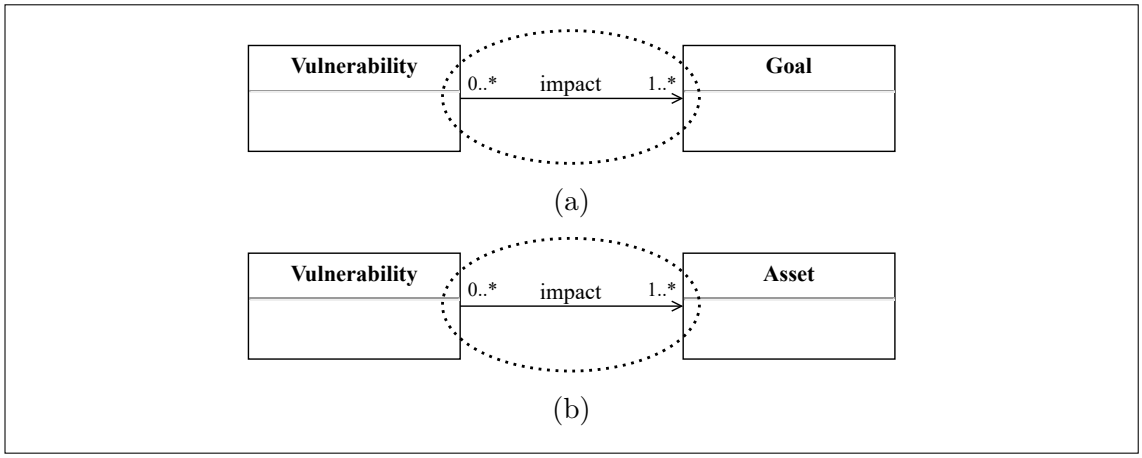


Figure 3.19: Impact relationship

3.4.7 Include

The Include association highlights the relationship between an Actor class and Goal, Asset and Constraint classes. Figure 3.20a and 3.20b shows a unidirectional *include* relationship drew as a solid line with an open arrowhead pointing to a Goal and Constraint class. Figure 3.20c shows a unidirectional *include* relationship drew as a solid line with an open arrowhead pointing to an Actor from an Asset class.

The multiplicity of an Actor to a Goal is [1..*], which indicates an actor may have at least one goal or many goals within the organisation. Similarly, a cardinality association between a Goal class to an Actor class is [1..*], which may be fulfilled by at least one or many actors.

The multiplicity of an Actor to a Constraint is [0..*], which shows an actor may have no constraint or expect many constraints from the organisation. On the other hand, a cardinality association between a Constraint class and an Actor class is [1..*], which has at least one or many actors.

The multiplicity of an Asset to an Actor is [1..*], which shows an asset has at least one or many responsible actors. On the other hand, a cardinality association between an Actor class to an Asset is [0..*], which describes an actor may have none or many assets.

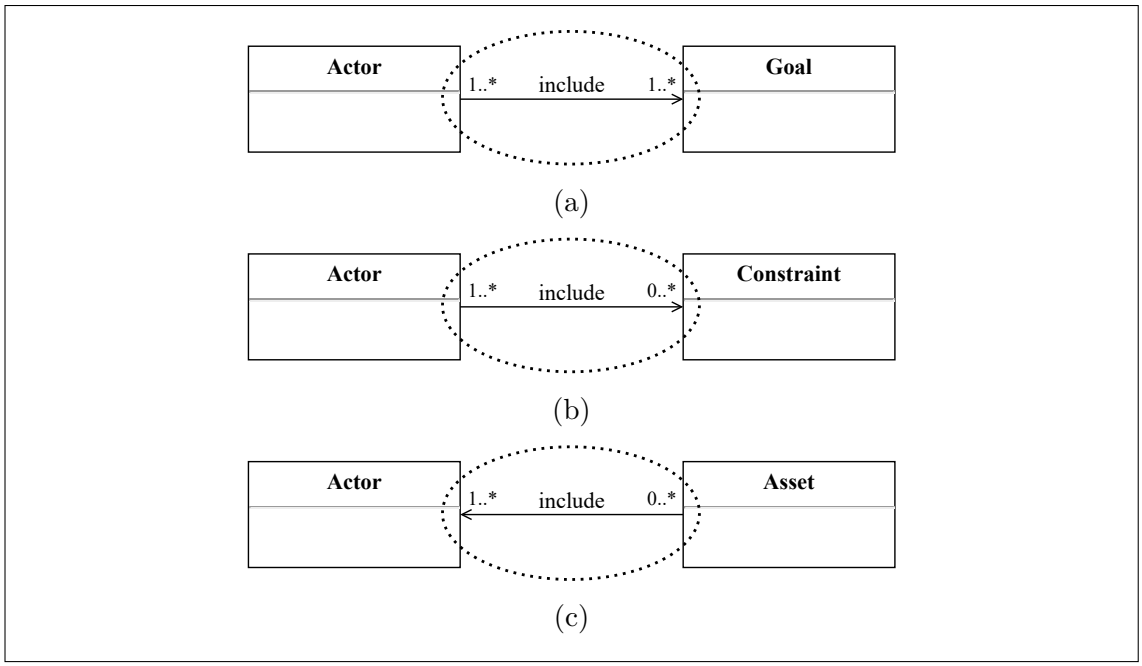


Figure 3.20: Include relationship

3.4.8 Mitigate

The Mitigate association describes the alleviation of a Treatment class on an information security risk. Figure 3.21 depicts a unidirectional *mitigate* association drew as a solid line with an open arrowhead pointing from a Treatment to risk.

The multiplicity between a Treatment to risk is [1..*], indicative of a treatment plan is capable of reducing one or many risks. A cardinality of risk towards a Treatment is [1..*], which indicates a risk could reduce to an acceptable level by one or many treatments.

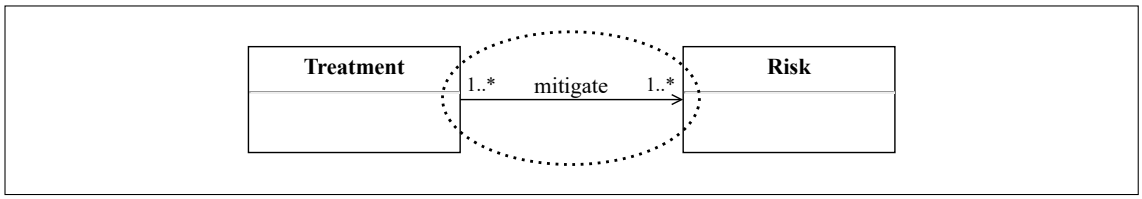


Figure 3.21: Mitigate relationship

3.4.9 Restrict

The Restrict association sets out the conceptual boundary from a Constraint class to a Goal and/or Asset class. Figure 3.22a depicts a unidirectional *restrict* association drew as a solid line with an open arrowhead pointing from a Constraint class to a Goal class. A similar demonstration is shown in Figure 3.22b for associating a Constraint to an Asset.

The association multiplicity between a Constraint class to a Goal or Asset class is [0..*], indicative of a constraint does not apply to any goal or asset, while it could restrict as many goals or assets. Also, a Goal and Asset association cardinality towards a Constraint is [0..*], which indicates that they could have no restriction from any constraints or more than one.

3.4.10 Satisfy

A constraint should be satisfied by at least one objective. The Satisfy relationship highlights the fulfilment of a constraint from a defined objective. Figure 3.23 shows a unidirectional *satisfy* relationship drew as a solid line with an open arrowhead pointing to a Constraint class from an Objective class.

The multiplicity of an Objective to a Constraint is [0..*], which indicates a particular objective may satisfy none or many constraints. On the other hand, a cardinality relationship from a Constraint to an Objective is [1..*], which a constraint has at least one or many corresponding objectives to be fulfilled.

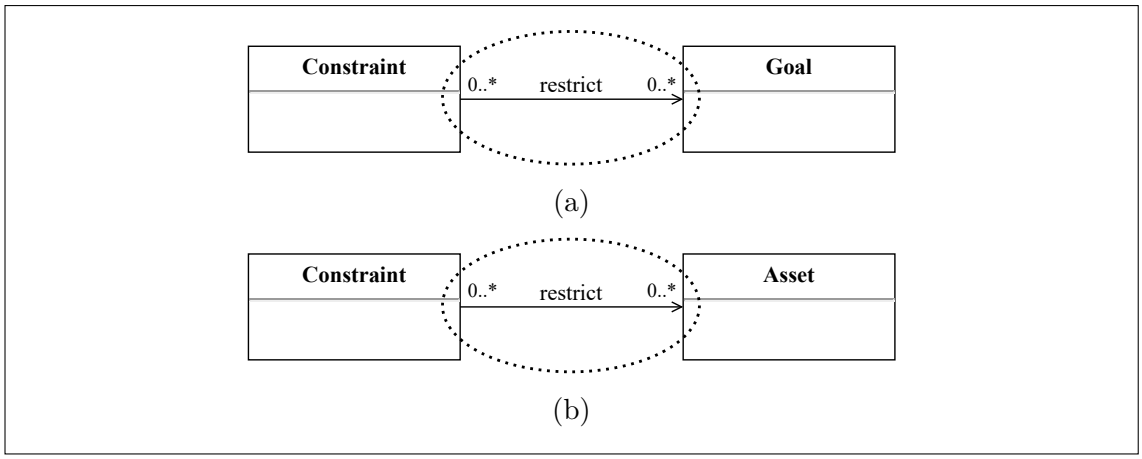


Figure 3.22: Restrict relationship

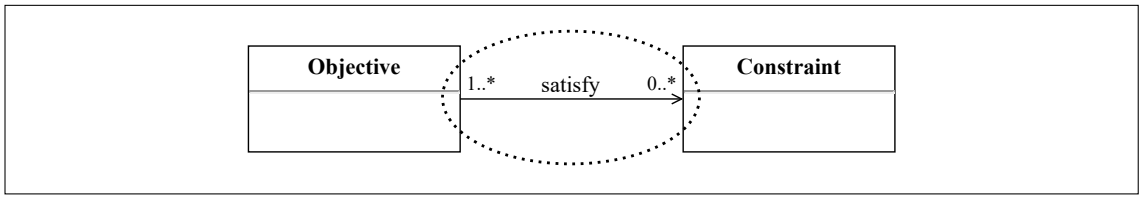


Figure 3.23: Satisfy relationship

3.5 Summary

This chapter introduced the INFORMS modelling language by extending concepts from goal-oriented requirements engineering to describe the requirements of the ISO/IEC 27001 standard. It presented the meta-model for the modelling language along with a detailed description of each concept. Also, each concept described with their attributes and operations. Finally, it examined the relationships between the concepts of the modelling language.

Chapter 4

INFORMS Framework

The investigation of the literature identified significant concerns for organisations in implementing the ISMS; hence, a framework introduced to support the design and implementation of the information security management systems. The final output resulting from the application of this framework is a system process containing both functional and security implementing activities. The remaining part of this chapter presents the INFORMS framework; a description of the framework work-flow and its structure will be explained. Finally, each view in the framework will be discussed.

4.1 Framework Overview

The modelling language and its concepts show the static structure of ISMS. The modelling language on its own helps to understand the overall structure of the standard; however, it does not support the implementation of ISMS as required by organisations.

The INFORMS framework presents a selection of relationships which can be used to integrate the organisation architecture with the elements of the standard. Apart from facilitating the elicitation of information security requirements, it also provides a means of producing the ISMS processes via a set of model and activities.

The graphical presentation [1] of the framework is portrayed in a graphic diagram shown in Figure 4.1. The framework provides a coherent set of activities, known as *viewpoint*, when populated, provide a graphical and textual visualisation of the organisation implementing ISMS. The figure illustrates the relationship between the five INFORMS Viewpoints, in particular, the way that the Strategic, Operational, Technical Viewpoints have a layers relationship. The System Viewpoint sits beneath the Strategic Viewpoint and has a supporting role across the Operational and Tech-

[1]The overall shape and graphical presentation of the framework inspired by the analysis of Ministry of Defence Architecture Framework and The Department of Defense Architecture Framework.

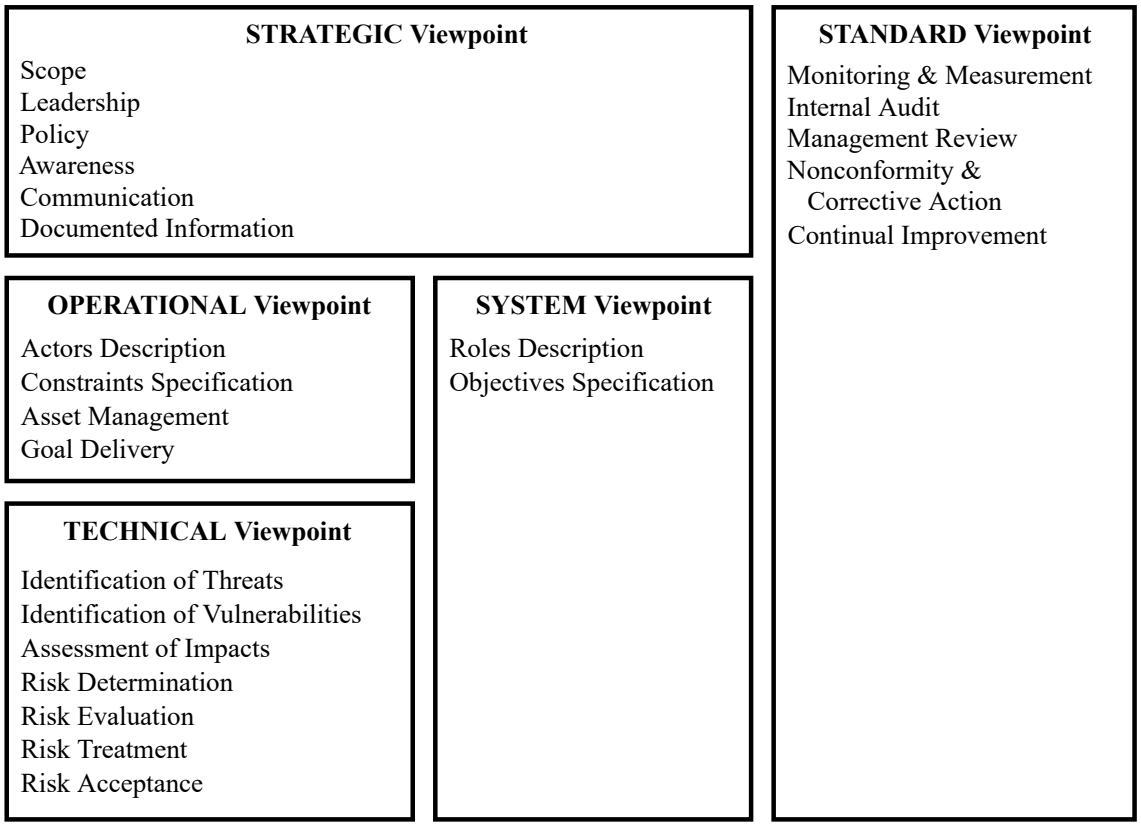


Figure 4.1: INFORMS framework

nical Viewpoints. The Standard Viewpoint sits alongside the others on supporting the requirements of the standard. Each viewpoint has a particular purpose, and usually presents one or combinations of the following:

- Broad summary information about the whole organisation, e.g., strategic.
- Narrowly focused information for a specialist purpose, e.g., technical, standard.
- Information about how aspects of the organisation are connected, e.g., operational, system.

One of the principal objectives is to present this information in a way that is understandable to the many stakeholder communities involved in developing, delivering, and sustaining capabilities in support of the organisation's mission. It does so by dividing the problem space into manageable pieces, according to the stakeholders' viewpoint. Each viewpoint takes a different perspective on the integration of business processes with the requirements of the ISMS. Each viewpoint is a collection of several Views, which describes diverse but consistent details within a particular viewpoint.

It structures implementers' thinking by dividing the organisation description into various views and offer modelling framework for documenting each view. It allows for making systemic design approach on all areas of the organisation. For instance, within the Operational Viewpoint, the Asset Management View provides insight

into the governance of the organisation's resources, while Goal Delivery captures the conceptual goals of the organisation.

The *view* is a specification of a way to present an aspect of the architecture. The information produced from one view interacts and flows within the corresponding viewpoint or other viewpoints in the framework. For example, the Asset Management View in the Operational Viewpoint identifies the risk owner for each information assets, and such information will be used in the Risk Acceptance View in the Technical Viewpoint.

Each group of users within the INFORMS could have different needs and populate the INFORMS Viewpoints that are of relevance to them. It means that most of the users of the framework only deal with the population and exploitation of a subset of the INFORMS Viewpoints, and few need to understand and deal with all the viewpoints in INFORMS.

The data produced from each view adds richness to the overall description of the architecture and strength the whole description of the ISMS. Since INFORMS is a module-based approach, each viewpoint is independent while most views must be completed at a particular point during the implementation process. On the other hand, if the organisation aim to certify with the ISO/IEC 27001, it is required to complete and fulfil all the views in the framework.

An architectural description at each viewpoint varies in content, structure, and level of detail. Tailoring the architectural description development to address specific, well-articulated, and understood purposes help to collect the relevant data at the appropriate level of detail to support specific decisions or requirement. The viewpoints structured into five categories:

Strategic Viewpoint defines the desired business vision for introducing the ISMS and baselines for effective delivery of the ISMS. It consists of six views, including:

- Scope: the extent of the boundaries and applicability of the ISMS.
- Leadership: top management's commitment and overall responsibility for the ISMS.
- Policy: top management's direction and aims for information security appropriate to the purpose of the organisation.
- Awareness: information security awareness and education programme to inform all actors of their information security obligations.
- Communication: systemic approach to provide, share or obtain information between organisation and actors.
- Documented Information: methodical process to create, update, and control documented information for the requirements of the standard.

Operational Viewpoint defines the processes, information and entities included in the scope of the ISMS. It consists of four views, including:

- Actors Description: identification and description of each actor relevant to the purpose of the organisation.
- Constraints Specification: understanding the boundaries and restriction of assets and goals introduced by the expectation of actors.
- Asset Management: organised process to the governance and recognition of information assets.
- Goal Delivery: a businesslike approach to manage and deliver the strategic interest of actors.

Technical Viewpoint defines the technical nature of information security and speculation of risks towards the views in the Operational Viewpoint. It consists of seven views, including:

- Identification of Threats: recognition of unwanted incidents and threats to information assets and goals.
- Identification of Vulnerabilities: recognition of assets and goals' weaknesses.
- Assessment of Impacts: analysis of consequences in the event of risk.
- Risk Determination: methodical approach to undertake analysis of risk in varying degrees of detail.
- Risk Evaluation: analysis of risks in comparison against risk evaluation criteria and risk acceptance criteria.
- Risk Treatment: defining a risk treatment plan.
- Risk Acceptance: analysis of decisions to accept risks.

System Viewpoint defines the interconnection between the processes of the organisation and the requirement of the standard. It consists of two views, including:

- Roles Description: defining roles to fulfil designated responsibilities.
- Objectives Specification: description of operational aims to achieve the information security policy.

Standard Viewpoint defines and articulates the organisation's performance to comply with the requirements of the standard. It consists of five views, including:

- Monitoring and Measurement: assessment of information security performance and effectiveness of the ISMS.
- Internal Audit: independent and planned analysis of ISMS effectiveness.
- Management Review: top management evaluation of ISMS.
- Nonconformity and Corrective Action: identification of non-conformities.
- Continual Improvement: capability planning to improve ISMS.

Additionally, Figure 4.2 provides a mapping between the clauses of the standard and views of the INFORMS. Note that an association between the standard and the framework's views should not be interpreted as indicating that the views are fully compliant with all the clauses of the standard; further detail would be needed to confirm the level of conformity.

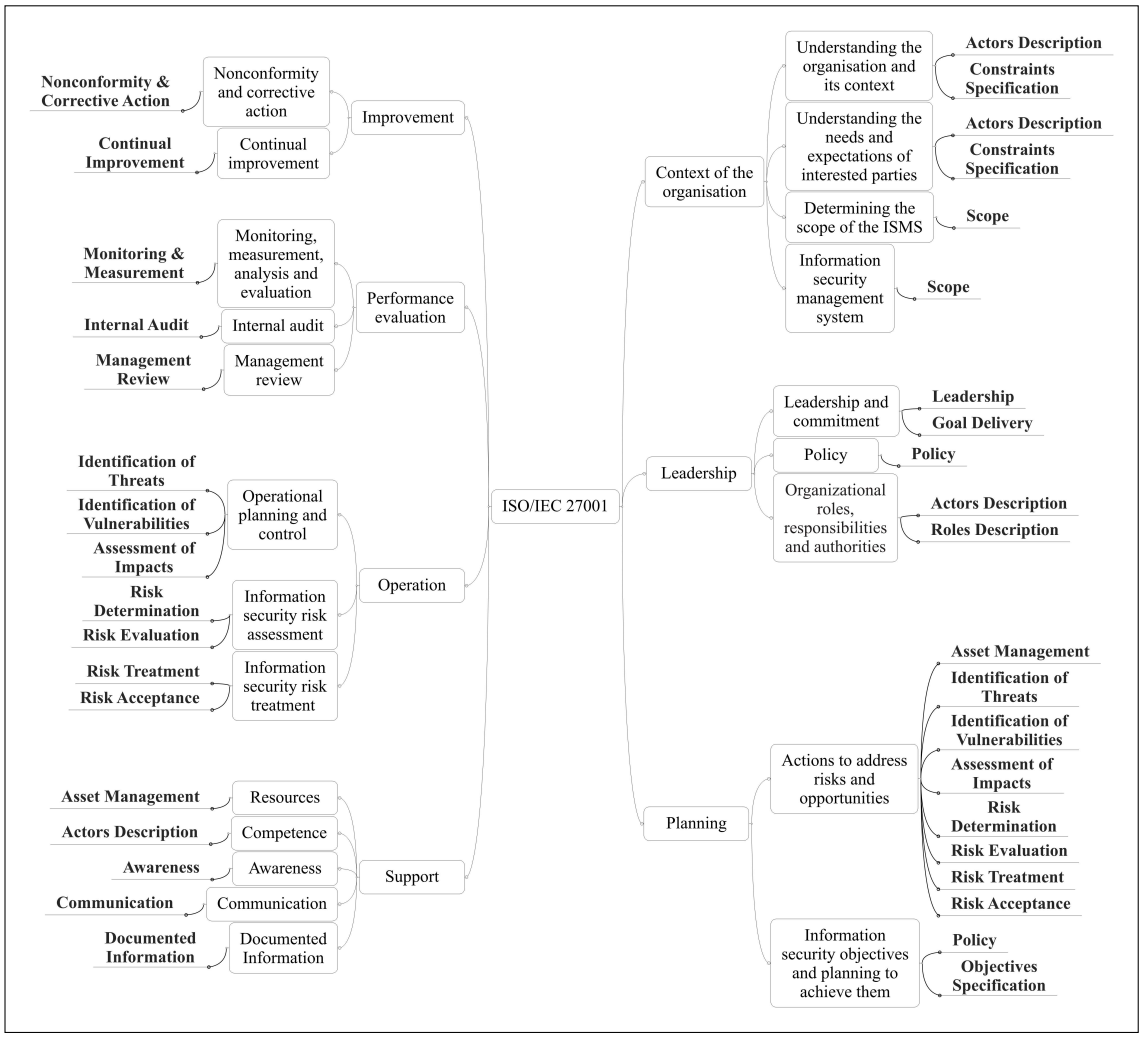


Figure 4.2: Mapping of ISO/IEC 27001 to INFORMS

4.1.1 Framework Workflow

The INFORMS framework developed as coherent, contiguous models that when viewed as a whole present a complete picture of ISMS. INFORMS modelling language defines a rich selection of relationships which used to integrate the various elements of the standard. The framework is intended for any organisation to implement an ISMS; the audience mainly include:

– *System implementers* who need to correctly interpret and model the requirements of the standard provided to them and need guidance on the creation of

the ISMS.

- *Top management* need to understand the overall expectation of the ISMS to provide resources and support to comply with the standard appropriately.
- *Middle management* to understand the detailed requirements of the standard to prepare and provide gap analysis in the readiness of their area of work.
- *Internal auditor* uses the created models to satisfy the suitability and effectiveness of the scope of an audit and provide suggestions on the nonconformities.
- *External auditor* may use the created models to understand the overall picture of the organisation's ISMS and work it through the first stage audit or gap analysis.
- *Tool developers* and engineers who are implementing management system repositories for storing and manipulating the requirements of the standard.
- *Trainers and educators* who require reference material to teach and support ISMS implementation.

Implementing and maintaining an ISMS is a teamwork effort amongst various layers of the organisation and rarely the work of one person, and it is useful to be able to logically divide architecture into domains, each concerned with one aspect of how the ISMS works in an organisation. It also proves useful when publishing architecture to different stakeholders, e.g., Auditors.

For this reason, INFORMS defines a set of viewpoints with each takes a different perspective upon the whole structure of ISMS. It demonstrates a businesslike approach to identify and pinpoint the failure of ISMS implementation. The process emphasises on data and relationships among and between data. This approach ensures concordance between views in the architectural while ensuring that all essential relationships captured to support a wide variety of analysis tasks. The views created as a result of the architecture development process provide visual renderings of the underlying architectural data and convey information of interest from domains needed by specific user communities or decision-makers. The working relationship between the viewpoints and their interconnected concepts of the INFORMS is presented in Figure 4.3.

Strategic Viewpoint is the first phase of the framework with an aim to align the organisation's strategy with ISMS. While this viewpoint has no corresponding concepts from the modelling language, however, it refers to the operations of the concepts in the language, e.g., Documented Information. The Strategic Viewpoint and its views are set out in Section 4.2.

Operational Viewpoint is the second phase of the proposed framework and aims to capture the security requirements of an organisation. This viewpoint incorporates

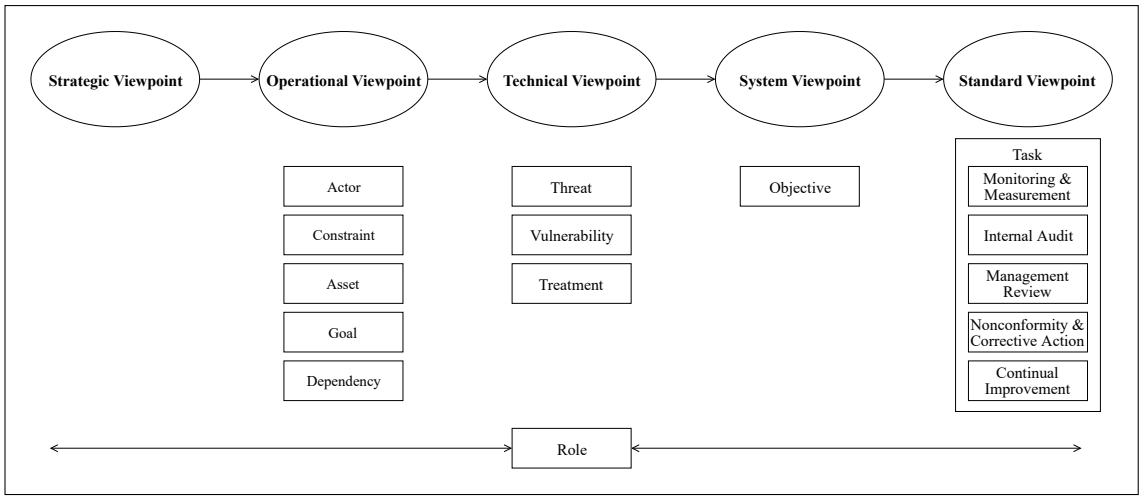


Figure 4.3: Workflow of INFORMS framework

four concepts and one relationship from the modelling language, including Actor, Constraint, Goal, Asset, and Dependency. A detailed description of the Operational Viewpoint and its concepts are described in Section 4.3.

Technical Viewpoint is the third phase in the framework which performs the risk management, and it enables to understand better the impacts of the information security risks on the organisational goals and assets identified in the previous phase. This phase includes related activities which include concepts such as Threat, Vulnerability, and Treatment. The Technical Viewpoint and its views are described in Section 4.4

System Viewpoint is the fourth phase in the framework which defines the specific purposes for implementing information security management systems, e.g., confidentiality, integrity, and availability. This viewpoint includes concepts like Objective and Role. The latter is accessible from other views in the framework. System Viewpoint's views are described in Section 4.5

Standard Viewpoint is the fifth and final stage of the framework that mainly involves with analysis of the requirements of the standard to ensure that concepts processed in the previous viewpoints are suitable and effective. This viewpoint is consist of Task concept which incorporate its attributes in a series of linked views such as Monitoring and Measurement, Internal audit, Management review, Nonconformity and Corrective Actions, and Continual Improvement. A detailed breakdown of the Standard Viewpoint is described in Section 4.6

4.1.2 Presentation

The analysis and implementation of an ISMS produce a series of information and records that it can be overwhelming to decision-makers when presented in a raw

format. Likewise, many of the structured methodologies of the studies identified in the literature are unwieldy because of their format and are suitable for trained or expert users.

The implementation process and outputs from ISMS need to be presentable to non-expert decision-makers in organisations that may not have technical training in the development, e.g., top management. The presentation of output from each viewpoint is a logical extension of the overall process. The presentation techniques proposed according to the idea that business information, captured both internally and externally to an organisation's architecture in support of user requirements, can be displayed in a way that enhances clarity, understanding, and facilitates decision-making. That often means complex technical information has to translate into a presentation method that is useful to the user.

The output from the views could be presented as documents, tables, or graphical representations and serve as a template for organising and displaying data in a more easily understood format to aid the decision-maker and process owners. The presentation of views shown in Table 4.1 are categorised into the following types:

- Graphical: visualising data accomplished through the INFORMS modelling language graphical notations and concepts describing the structural or behavioural aspects of a system.
- Tabular: data arranged in rows and columns, which generally amplify or have a direct relationship to the behavioural models.
- Text: presenting data in the form of words, sentences and paragraphs. While the graphical presentation of data is the most popular and widely used in the framework, the textual presentation allows the implementers to present qualitative data that cannot show in graphical or tabular forms.

The view's output should transfer the collected information and present in a manner depicting traceability to other views and activities in the ISMS for the use of various audiences. This is determined through the requirements of the standard and facilitated by data collection methods employed during the INFORMS process. This step can often simplify through reuse of data previously collected by other implementers, but relevant to the current effort.

Presentation of views is always dependent on the quality of the architectural information collected. The presentation techniques do not intend to cover all the details produced in the implementation of ISMS, e.g., a Management Review View is modelled using the INFORMS modelling language to support the requirements of the standard; however, additional details may be necessary or be produced by the organisation to enable the aspects of decision-making in having an effective ISMS.

Table 4.1: Methods in presenting views

View	INFORMS	Tabulation	Text
Scope			+
Leadership			+
Policy			+
Awareness		+	
Communication	+		+
Documented Information	+	+	+
Actors Description	+	+	
Constraints Specification	+		
Asset Management	+	+	
Goal Delivery	+		
Dependency Provision	+		
Identification of Threats	+		
Identification of Vulnerabilities	+		
Assessment of Impacts	+	+	
Risk Determination	+	+	
Risk Evaluation	+	+	
Risk Treatment	+	+	
Risk Acceptance	+	+	
Roles Description	+		
Objectives Specification	+	+	
Monitoring & Measurement	+		
Internal Audit	+		
Management Review	+		
Nonconformity & Corrective Action	+		
Continual Improvement	+		

4.1.3 General Structure of Views

In having a disciplined process for the use of views, the framework produces quality results, not be prone to misinterpretations, and therefore, be of high value to decision-makers and implementers. INFORMS uses an identical pattern for describing and use of each view to describe the processes in the framework. A typical pattern for each view explained in below includes a UML activity diagram, input, description of the activity, output, and normative references.

Activity Diagram using UML notations are drawn for each view to visually indicate the steps and processes that are required to fulfil a particular view. All views

except those in the Strategic Viewpoint includes an activity diagram to illustrate the process of each view. A collection of activity diagram notations used to demonstrate the views of the framework are presented in Figure 4.4. In between the Initial node and the Activity final node are other nodes and connectors which briefly explained in below [118, 119].

- Initial node: a control node is shown as a solid circle at which flow starts when the activity is invoked.
- Fork: a control node is shown as a line segment that splits a flow into multiple concurrent flows. It supports parallelism in activities and has one incoming flow and several outgoing parallel flows.
- Object: an activity edge that can have objects or data passing along it.
- Join: It has multiple incoming edges and one outgoing edge to indicate that all incoming actions must finish before the flow can proceed past the join. The notation for a join node is a line segment.
- Action: an activity specifies the executions of subordinate behaviours using a control and data flow model. Actions notated as round-cornered rectangles with the name or description of the action placed inside of the rectangle.
- Input/output pin: an object node for inputs and outputs to actions shown as a small rectangle attached to the action rectangle with its name displayed near the pin. Input pin means that the object is input to action while the output pin is output from an action.

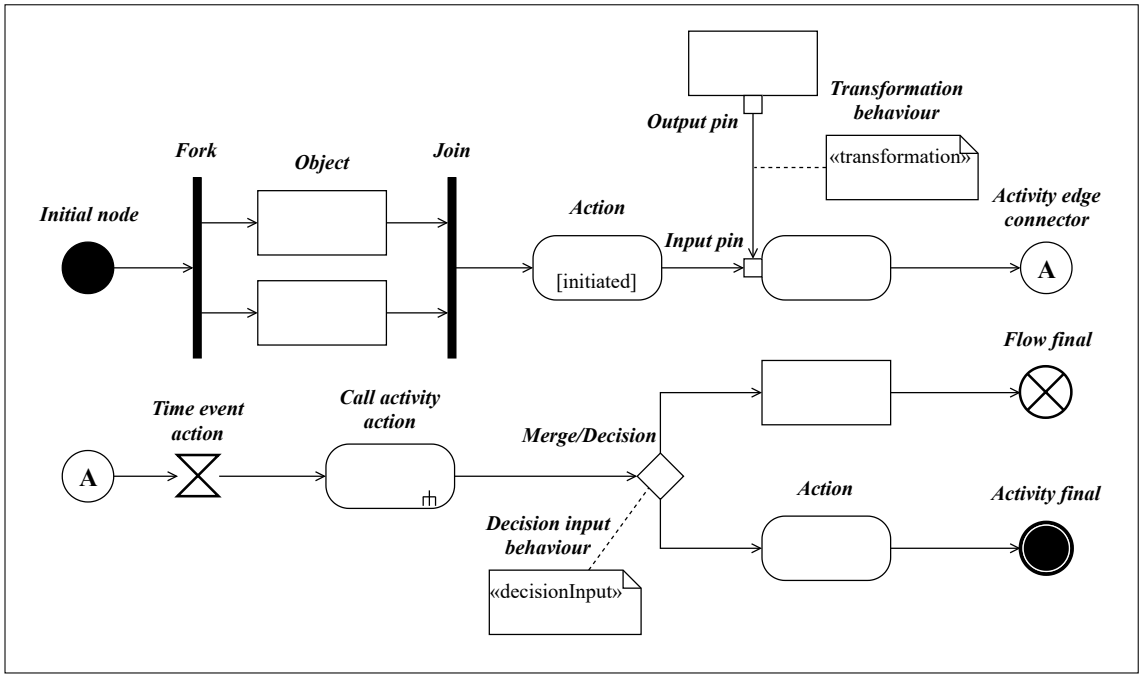


Figure 4.4: UML activity digram notations

- Transformation behaviour: it shows where input parameters come from as if a query were being performed. A transformation behaviour is shown as notes attached to the invocation with the keywords ≪transformation≫.
- Activity edge connector: it is a small circle indicating a name of the edge as a notation. The circles and lines involved map to a single activity edge in the model. Every connector with a given label is paired with exactly one other with the same label on the same activity diagram.
- Time event action: a time event specifies a point in time by an expression. The time event action is notated with an hourglass.
- Call activity action: a miniature hierarchy, indicating that this invocation starts another activity that represents a further decomposition. The execution of a single action may induce the execution of many other actions. The call activity action is indicated by placing a rake-style symbol within the action.
- Merge/Decision: decision nodes introduced to support conditionals in activities to avoid redundant recalculations in guards. A merge node is a control node that brings together multiple alternate flows and a single activity edge leaving it. The functionality of the merge node and decision node can combine by using the same node symbol, shown as a diamond-shaped symbol.
- Decision input behaviour: decision can have decision input behaviour specified by the keyword ≪decisionInput≫ and some decision behaviour or condition placed in a note symbol and attached to the appropriate decision node.
- Flow final: a flow final node is a final node that terminates its path, not the whole activity. It is presented as a small circle with X inside.
- Activity final: It marks the end of an activity shown as a solid circle with a hollow circle.

Input describes the starting point, such as the existence of a decision or outputs from other views described in the framework. An input either refers to a complete output or a specific process from other views.

Activity is a detailed description of the application of a view; it provides a step by step explanation on how to implement a view. It guides with an illustration of an activity diagram to help with visualisation of the steps in using a view.

Output describes the result(s) or deliverable(s), upon completion of an activity, for example, a single or combination of presentation techniques described in the Section 4.1.2 and/or a list of processes or records in the organisation.

Normative References refer to the specific clause(s) and sub-clause(s) of the standard that is addressed by a view.

4.2 Strategic Viewpoint

The Strategic Viewpoint determines a strategic foundation led by the top management for the ISMS. The views introduced in the Strategic Viewpoint captures the organisation vision, policies, supports for the information security and overall commitment of top management to deliver a successful ISMS.

Strategic Viewpoint defines the desired business outcome and the contribution required from the top management to achieve effective implementation of the ISMS, i.e., it provides a means to align an enterprise's strategy with the activities required to deliver that strategy.

The views in the Strategic Viewpoint are high-level and describe the foundation of the ISMS and policies using terminology that is easily understood by non-technical users of the framework, which may include the use of terminology and acronyms routinely used in organisations. It provides a set of views that captures the enterprise scope for the ISMS, information security policy and concepts related to the operation of the ISMS. The six views that constitute the Standard Viewpoint describes below.

4.2.1 Scope

The scope of the management system is a precise definition of the physical and abstract boundary of the ISMS implementation and applicability of the management system requirements. Establishing the scope of an ISMS is a groundwork for the expansion of every other activity in the ISMS.

Input

(i) overview of high-level business requirements

(ii) the organisation's purposes for developing and conforming with the standard

Activity

An in-depth understanding of an organisation's interfaces and dependencies supports the decision making to include one or more particular processes, functions, services, locations, and legal entity in determining the appropriate scope for the ISMS. It defines where and for what precisely the ISMS is applicable as well as describing where and for what it is not.

The scope defines the boundaries that establish the depth and breadth of ISMS in an organisation, helps define its context and level of detail required for the overall content of the ISMS. The essential concept for this view is the clarity of the scope defined for the ISMS. The top manager has the primary responsibility to define a precise and suitable scope to ensure the ISMS can successfully achieve its objectives.

The activities with the impact on the ISMS should be considered in the scope, including those that are outsourced within the organisation or to independent sup-

pliers. A multi-step approach could be used to establish the scope of an ISMS, including:

- determine the preliminary scope;
- determine the refined scope;
- determine the final scope; and
- approval of the scope.

The scope of the management system may include the whole of the organisation or specific sections of the organisations. The readiness of the business activities to be included as part of the ISMS coverage is critical since immature business activities may inadvertently cause interruption to the overall readiness of the ISMS. On the other hand, it worth to note that all functions that are necessary to support the activities of the ISMS can affect the determination of the scope even though not included in the scope of the ISMS.

Output

(i) description of the ISMS scope

Normative references

(i) clause 4.3

(ii) clause 4.4

4.2.2 Leadership

Top management is "a person or group of people who directs and controls an organisation at the highest level" [120]. The top management shall demonstrate commitment by taking accountability for the effectiveness of the ISMS.

Input

(i) Top management approval for initiating an ISMS

Activity

Leadership's commitment is a prerequisite for an effective ISMS. The top management has the overall responsibility for the ISMS, including directing the ISMS, allocating the budgets and providing resources, and assigning responsibilities and authorities to manage the operation of the ISMS.

Successful implementation of the ISMS and full conformity to all requirements of the standard may take up to two years; hence, it needs the top management's commitment to ensure the requirements of the standard seemingly integrates with the processes of the organisation. The top management should display its commitment by its direct participation and lead by example in some regions of the ISMS, including:

- Information security policy: ensuring information security policy is established

and is compatible with the strategic direction of the organisation.

- Information security objective: ensuring information security objectives are identified and are consistent with the information security policy.
- ISMS integration: ensuring the requirements of the ISMS and identified controls incorporates into organisation processes. Top management should support process owners in consolidating changes in processes and controls.
- Resource availability: providing resources inclusive of financial, personnel, facilities and technical infrastructure for an effective ISMS. The resources should be available throughout the ISMS life cycle and be appropriate to the organisation's context, such as the size, the complexity, and constraints of the ISMS.
- Communication: imparting the significance of the ISMS and conforming to the requirements of the ISMS by giving practical examples in the context of the organisation.
- Practical collaboration: ensure the information security processes implemented as expected by the requirements of the standard and organisation's requirements to achieve the ISMS intended outcomes. Top management should participate by reviewing the status of the ISMS effectiveness derived from measurements, audit and management reviews.
- Promote awareness: ensuring persons in the organisation are aware of their impact on the performance of the ISMS, for example, top management could be an exemplary role and provide feedback to personnel on the alignment of organisation's strategic goals with the ISMS.
- Promoting continual improvement: top management's engagement in the management review meetings should highlight the performance of the ISMS and set objectives for continual improvement.
- Roles and authorities: supporting the ISMS by encouraging the roles assigned to the ISMS activities.

Output

(i) top management commitment to allocate resources for the delivery of the ISMS

(ii) top management participation in leadership activities of the ISMS, e.g., management review meetings

Normative references

(i) Clause 5.1

4.2.3 Policy

The information security policy is the proposed strategy by the top management for the direction of the organisation's information security. It highlights the importance

of the ISMS by describing the specific needs of the information security for the organisation.

Input

(i) output from Scope View

(ii) organisation's priorities to develop an ISMS

Activity

The information security policy is the primary direction in setting information activities and inception for alignment of other policies, procedures, activities and objectives related to information security.

The information security policy should be aim-oriented and serve the purpose of the organisation; it should align with the organisation's culture, nature of activity, issues and concerns related to the information security. The policy should be written in a format and language appropriate for being communicated to the interested parties within the scope of the ISMS.

The policy partially derives its mandate from the information security objectives (see Section 4.5.2); hence, the top management should include objectives or propose the framework for setting those objectives in the information security policy. Additionally, the top management should demonstrate its commitment to meet the requirements related to information security, including continual improvement of the ISMS.

Output

(i) a document describing information security policy

Normative references

(i) Clause 5.2

4.2.4 Awareness

Awareness relates to set of planned programs developed by the organisation for actors doing work under the organisation's control to understand their responsibilities and how their behaviour contributes to the effectiveness and performance of the ISMS. The graphical notation for modelling awareness is illustrated in Figure 4.5 as a rectangle with double-struck vertical edges with the letters *AW*.

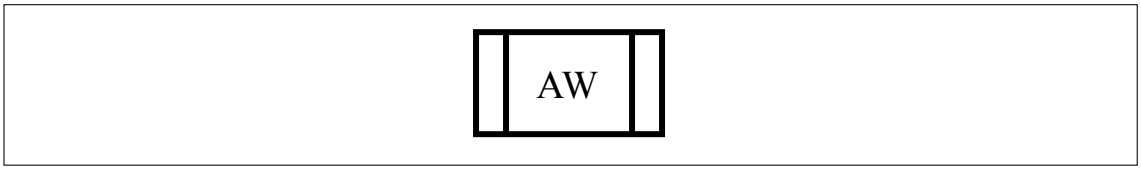


Figure 4.5: Awareness graphical notation

Input

(i) output from Policy View

Activity

A security awareness program is a formal program with the goal of training users of the potential threats to an organisation's information and how to avoid a situation that might put the organisation's data at risk. The goals of the security awareness program are to lower the organisation's attack surface, to empower users to take personal responsibility for protecting the organisation's information, and to enforce the policies and procedures the organisation has in place to protect its data [121].

Information security awareness is the stakeholder knowledge and attitude within an organisation to protect their information assets from any possible security breach. The focus of information security awareness should be to achieve a long term shift in the attitude of employees towards security, whilst promoting a cultural and behavioural change within an organisation [122].

Awareness concerns actors doing work under the organisation's control who need to know, understand, accept the objectives of the information security policy and ensures that their contribution is aligned with such objectives to enhance the effectiveness of the ISMS. Actors should be aware that implications of not conforming to the requirements of the ISMS can harm information security or repercussions for the actor [123]. The organisation should:

- prepare a programme with the specific messages focused on each audience, e.g., internal and external actors;
- include information security expectations within the awareness materials;
- prepare a plan to communicate messages at planned intervals;
- verify the knowledge and understanding of messages from the awareness sessions to test knowledge transfer;
- verify whether persons act according to the communicated messages; and
- contact points and resources for additional information and advice on information security matters, including further information security awareness materials.

The awareness programme should be established in line with the organisation's information security policies and taking into consideration the actors' roles in the organisation, and where relevant, the organisation's expectation on the awareness of contractors. These requirements can include in the procedures they are expected to follow to do their job, e.g., call centres need to follow the security procedure of verifying customers before discussing an account information to maintain the confidentiality and integrity of the customer's information.

The awareness programme is consist of appropriate awareness-raising activities relevant to the information security procedures, such as campaigns and issuing booklets or newsletters. Awareness training can use different delivery media, including classroom-based, distance learning, web-based and self-paced.

The activities in the awareness programme should be scheduled overtime, preferably regularly so that the events are repeated and cover new employees and contractors. The awareness programme should also be updated periodically and to be built on lessons learnt from information security incidents.

Output

(i) list of activities for the awareness programs

(ii) roles and responsibilities for conducting awareness programs

Normative references

(i) Clause 7.3

4.2.5 Communication

Communication is a key process that an organisation conducts to provide, share or obtain information with internal and external actors to increase an actor's involvement with the context of the ISMS. The graphical notation for modelling Communication is illustrated in Figure 4.6 as a rectangle with double-struck vertical edges with the letters *CO*.

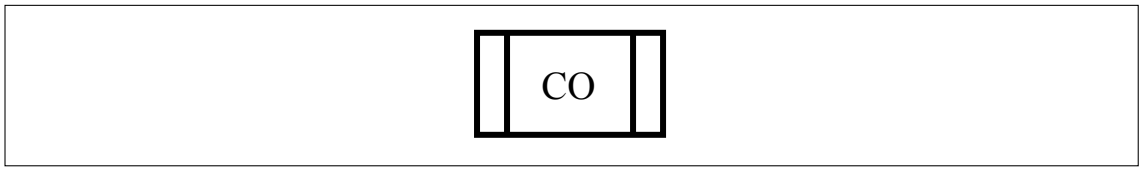


Figure 4.6: Communication graphical notation

Input

(i) output from Actors Description View

(ii) output from Constraints Specification View

Activity

The communication process relevant to information security management system could trigger between internal actors at all levels of the organisation or between the organisation and external actors. Such a process requires an extensive understanding of the:

– Content: extend of content needs to be communicated including plans and results of the risk management, information security objectives and successful completion of those objectives, incidents and crises notification that require mandatory communication to regulatory bodies, or organisation's re-

quirements to exchange information with interested parties to increase and preserve trust in the organisation capability.

- Interval: appropriate or obliged point in time for communication activities, the interval or frequency of the communication can happen periodically or as required.
- Recipient: understanding the audience and actors of communication activities. An appropriate method of communication should be identified to ensure the messages are sent, have been correctly received and understood by the recipients. The method should be protected from the loss of confidentiality and integrity of exchanged information.
- Role: responsible role in the organisation to launch the communication activities, e.g., public relations officer for communicating with external actors in the event of special cases or HR officer for internal communication.
- Impact: the processes to be affected by communication activities.

Output

(i) roles and responsibilities for conducting communication

(ii) identification of processes affected by the communication activities

Normative references

(i) Clause 7.4

4.2.6 Documented Information

The standard explicitly requires that the information produced by specific processes to be controlled and maintained by the organisation and be available as documented information. While the documented information and records are mandatory, there is supplementary documented information for the organisation to determine as being necessary for the effectiveness of the ISMS [70]. The graphical notation for modelling Documented Information is illustrated in Figure 4.7 as a rectangle with double-struck vertical edges with the letters *DI*.

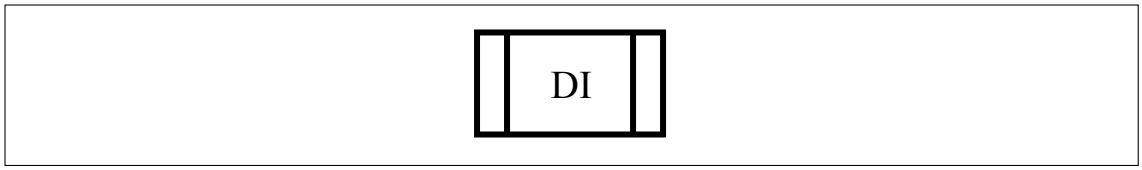


Figure 4.7: Documented Information graphical notation

Input

(i) output from the Scope View

Activity

Documented information is required for recording actions, decisions and outcome(s) of ISMS processes and information security controls. The extent of documented information for an ISMS can differ from one organisation to another due to the size of the organisation and its type of activities, the complexity of processes, and the competence of actors.

Documented information can contain information about information security objectives, risks, and information about processes and procedures to be followed. Many activities within the ISMS produce documented information that used as an input for another activity, e.g., Management Review View requires the outcomes of processes from the Risk Determination View. Overall, the mandatory and additional documented information should provide adequate input to conduct the evaluation of the ISMS in the Standard Viewpoint. Table 4.2 identifies a list of views that generates documented information or records as output.

Table 4.2: Documented information assignment

View	
Scope	Policy
Documented Information	Actors Description
Asset Management	Assessments of Impacts
Risk Determination	Risk Evaluation
Risk Treatment	Objectives Specification
Monitoring & Measurement	Internal Audit
Management Review	Nonconformity & Corrective Action

The ISO/IEC 27001 expects organisations to use a methodical approach to create and update documented information. These include criteria on how to:

- Identify and describe: the organisation should establish an approach for documented information to includes common attributes of every document, which allow clear and unique identification. These attributes may consist of the document type, the purpose and scope, title, date of publication, classification, reference number, version number, and revision history. The identification of the author and the person(s) currently responsible for the document.
- Format: statements and writing style should be tailored to the audience and scope of the documentation. Documented information may be produced and retained in any form, e.g., traditional documents, web pages, databases, computer logs, computer-generated reports, audio and video.
- Approve: appropriate management should take accountability for correctness,

suitability and adequacy of the documented information.

All of the documented information should classify in accordance with the organisation's classification scheme and should be protected and processed per its classification level. Documented information should be distributed and made available to authorised actors for each document information, and the means to use for distribution, access, retrieval and use. This should be in line with any requirements related to protecting and handling classified information.

The organisation should establish an appropriate retention period for documented information and ensure the information is legible throughout its retention period. The organisation needs to determine the disposition process at the expiry of the retention period of the documented information [124].

Output

(i) documented information required by the standard

(ii) documented information determined by the organisation as being necessary for the effectiveness of the ISMS

Normative references

(i) Clause 7.5

4.3 Operational Viewpoint

The Operational Viewpoint is represented in a series of interrelated views that depict organisational processes and their interaction within the context of the scope and information security policy established in the Strategic Viewpoint. Four views make up the Operational Viewpoint; all together highlight the corporate structure and capture the capabilities of the organisation. An outline of the Operational Viewpoint modelled using INFORMS modelling language to demonstrate the interrelation of the views is presented in Figure 4.8.

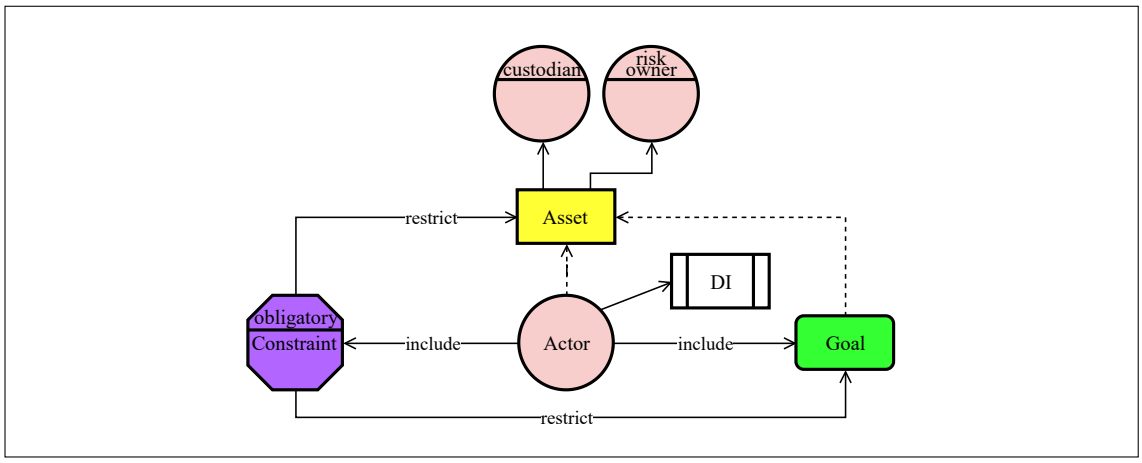


Figure 4.8: Outline of an Operational Viewpoint

4.3.1 Actors Description

Organisations shall identify the interested parties relevant to the ISMS. This view describes the concept of Actor, internal or external, and its relationships within the scope of the ISMS. Figure 4.9 shows the activity diagram demonstrating the processes involved in fulfilling the Actors Description View.

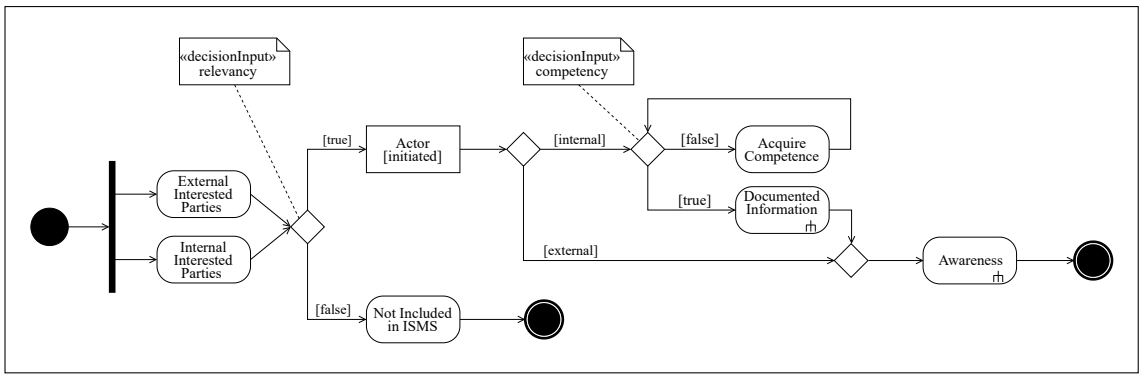


Figure 4.9: Activity diagram of Actors Description View

Input

(i) output from Scope View

(ii) list of internal interested parties who will benefit from the result of the ISMS

(iii) list of external interested parties who will benefit from the result of the ISMS

Activity

The implementation of ISMS provides contemplation to identify and integrate all interested parties into the information system. The correct identification of actors and their role within the organisation is a mandatory requirement of the standard. Determining the type of actors helps to anticipate the specific expectations of each actor related to information security. The organisation should regularly review the needs of actors to ensure that the actors and their requirements are relevant to the ISMS.

Internal actors can include decision-makers, process/information owners, support functions, personnel and users. External actors can consist of customers and consumers, shareholders, landlords, suppliers, outsourcing partners, competitors, regulators and legislators, and industry associations.

Another interested party who could be recognised in both types of actors is known as malicious actor or attacker. The existence of a malicious actor is a threat than an interested party for the organisation, i.e., organisations should consider actors by their *malicious capability* rather than their type or position. An external actor is not always a hacker, and an internal actor is not always a trusted party; therefore, organisations need to have a balanced approach for both internal and external actors.

A systematic assessment such as an information security risk management is required to examine and protect the organisation against all malignant actors.

For example, a member of top management could have administrative access to the information system since he/she is unlikely to be considered as a malicious actor nevertheless, the access right should have been allocated based on the organisation's User Access Management Policy. Given this, INFORMS has not introduced a separate type for a malicious actor to avoid further complexities and misinform in the implementation of an ISMS.

Another characteristic of an actor is its competency, which indicates the identification of the ability to apply the skills, training, and education needed to perform intended goals. An actor shall have the necessary competence for doing work under its control that affects the information security performances. Determining the necessary competence is mostly pertinent to the internal actors. However, a similar requirement of competency applies to the external actors who could be responsible for performing a goal which could affect the information security performance.

Each actor needs to be considered individually, and as a whole participant to the ISMS, e.g., a new internal actor may not have sufficient training and knowledge about the undertaking duties and requires permanent supervision by another internal actor like a line manager. If the line manager is not available, the new actor puts the organisation at risk with the lack of skills and competency, which could affect the ISMS. Therefore, it is crucial for organisations to regularly review actors' competency to ensure that they have the necessary competence in performing their duties. In such circumstances, the top management should pledge the opportunities to ensure the actor(s) develop competency based on appropriate education, training, or expertise.

Output

(i) list of actors who are interested in the outcome of the ISMS
(ii) records of skills, training, experience, and qualification available as a documented information

Normative references

(i) clause 4.1
(ii) clause 4.2
(iii) clause 5.3
(iv) clause 7.2

4.3.2 Constraints Specification

This view specifies the issues, requirements, or expectations of the actors relevant to information security. Identification of constraints enables the organisation to plan and analyse the information system in which the organisation operates. An activity diagram shown in Figure 4.10 depicts the processes involved in fulfilling the Constraints Specification View.

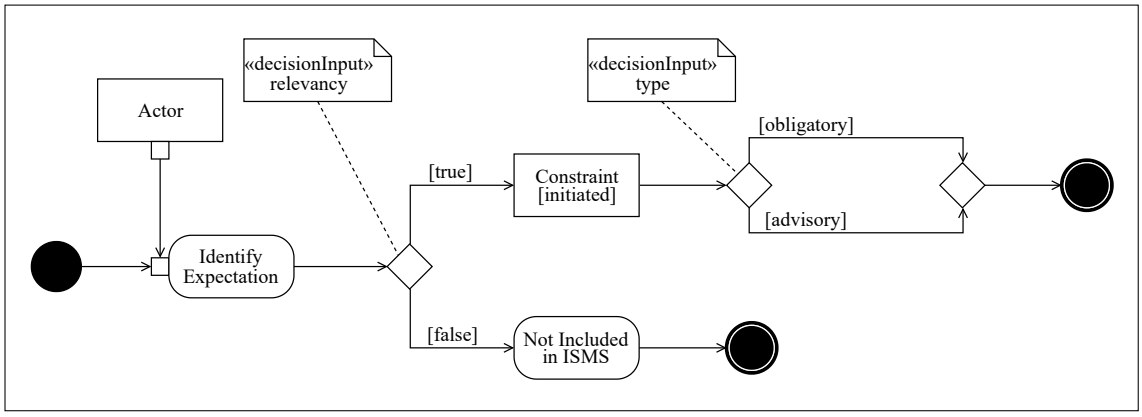


Figure 4.10: Activity diagram of Constraints Specification View

Input

(i) output from Actors Description View

(ii) expectations and requirements of the actors

(iii) overview of the internal and external issues

Activity

Constraint aims to identify the requirements and issues of the actors' related to information security, which could affect the organisation's ability to achieve the intended outcome(s) of its ISMS. Constraints are often beyond the control of an organisation and are conditions that an actor wish to introduce and impose to the ISMS.

Each actor has a number of requirements, and the organisation needs to identify those expectations and consider them in the implementation of the ISMS. Specifying constraint provides an opportunity to understand the actors better and take into consideration their issues and expectations, rather than a limitation to the information system. The analysis of the actors' requirements should include consideration to aspects such as social, cultural, political, legal, financial, technological, natural, and competitive.

The ISMS implementers may not have sufficient knowledge about the organisation's area of activities; thus, such a limitation could impact the accurate identification and analysis of the types of constraints. An organisation's top management,

legal advisor, financial and relevant business advisor, and security professionals are the most suitable candidates to specify constraints. This practice provides an additional opportunity for the top management to have a functional interaction with the implementation of ISMS.

Information security objectives shall consider the constraints and determine appropriate methods at relevant functions and levels to satisfy actors' requirements. Alternative approaches should be formulated to prioritise resources to those constraints that are critical to the ISMS. The selection of obligatory constraints depends on the organisation's specific priorities and situation. Advisory constraints should be considered by the organisation but satisfied if possible.

The organisation should continually analyse itself and its interaction with all actors to embrace opportunities to understand their requirements and expectation better. This continual review also helps to ensure that the information system adapts to changing constraints.

Output

(i) list of requirements, expectations and issues
(ii) list of corresponding actors to the constraints
(iii) identification of constraint types

Normative references

(i) clause 4.1
(ii) clause 4.2

4.3.3 Asset Management

Inventory of information assets is at the centre of the ISMS implementation. The organisation shall develop and maintain an inventory of information assets and information processing facilities as a prerequisite for adequate protection of assets. An activity diagram shown in Figure 4.11 illustrates the processes involved in fulfilling the Asset Management View.

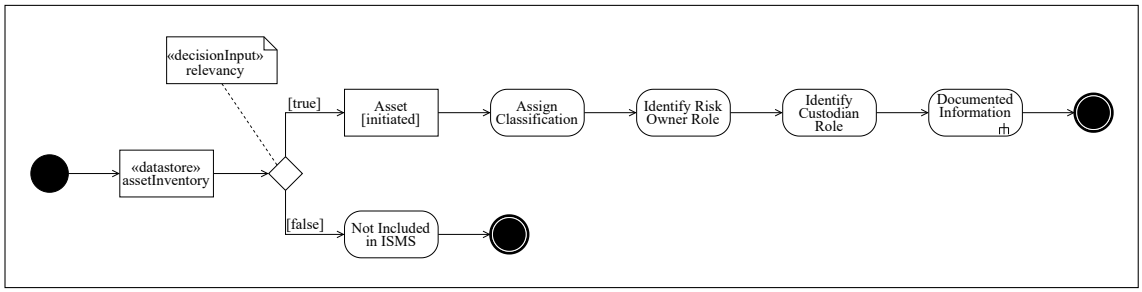


Figure 4.11: Activity diagram of Asset Management View

Input

(i) preliminary identification of information assets

Activity

Managing asset is a core activity of the Operational Viewpoint, and the correct identification of the assets ensures risks to information security are adequately managed. The asset inventory could be a detailed or generic description for each asset category; the organisation has the flexibility to implement the detail tailored to their need.

The asset inventory should be accurate, up to date, and consistent with other inventories in the organisation, e.g., finance, IT, HR. Each asset shall be assigned to a risk owner(s) at the creation of the assets or when assets are transferred to the organisation. The risk owner is responsible for the governance of the assigned assets over the whole asset lifecycle. The information lifecycle is an interconnected phase in managing the flow of information from creation following by processing, storage, transmission, deletion and destruction.

The risk owner is responsible for identifying an appropriate level of asset classification in accordance with the information classification scheme adopted by the organisation. Classification of assets should consider the business needs for sharing or restricting information, legal requirements, value, criticality and sensitivity of the asset. INFORMS incorporates levels of commercial information classification in three categories defined below.

- Public: information is not sensitive. Its disclosure and release would cause no damage to the organisation.
- Sensitive: information is considered personal in nature. It might include personally identifiable information and should be safeguarded against disclosure.
- Confidential: information is considered as the most sensitive. Its release or alteration could seriously affect or damage the organisation and requires the highest level of protection.

Additionally, the risk owner is responsible for identifying an appropriate asset custodian for safekeeping and overall maintenance of the asset over its lifecycle. Custodian is individuals as well as other entities having approved responsibility by the risk owner to oversight and have administrative and/or operational responsibility for an asset or group of assets. While the custodian is available to control and monitor the health of an asset, it is the asset owner who is accountable for the whole lifecycle of an asset.

Output

(i) list of organisational assets and other assets associated with information

(ii) corresponding risk owner

(iii) corresponding custodian

(iv) level of classifications

Normative references

(i) clause 6.1.2

(ii) clause 7.1

4.3.4 Goal Delivery

Organisations have a set of pre-defined procedures to achieve their strategic aims of the business; each procedure assigns to appropriate and relevant actors. An activity diagram shown in Figure 4.12 demonstrates the processes involved in fulfilling the Goal Delivery View.

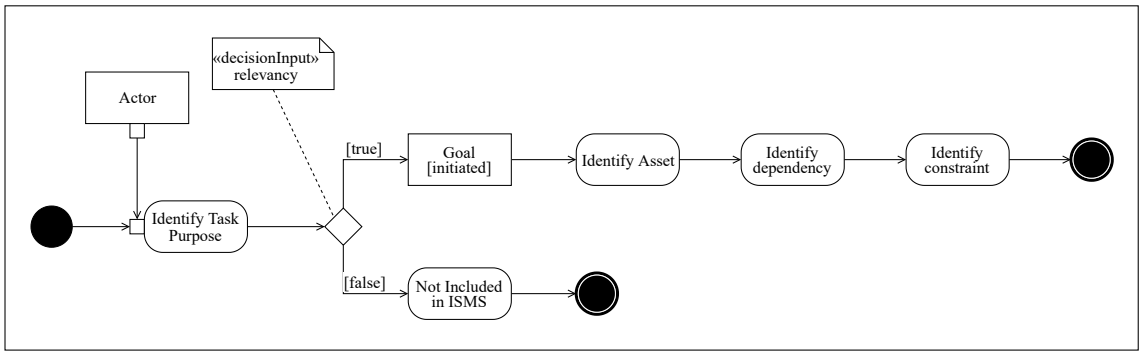


Figure 4.12: Activity diagram of Goal Delivery View

Input

(i) output from Actors Description View

(ii) preliminary duties of actors related to information systems

Activity

Each actor participates with an organisation to fulfil a business activity or has an interest in the overall business activity of the organisation, e.g., an IT technician provides support to maintain the operation of servers and a client benefits from a particular service provided by the organisation. Those activities, irrespective of an actor's type and nature of interest could be relevant to the scope of the ISMS.

It is the responsibility of the organisation to establish and interpret business activities into goals. Description of goals could be very detailed and exhaustive like *to repair out of service HP printers in the sales department* or could be an outline of a strategic goal such as *to provide a secure environment*. An assessment of each goal should be carried out to identify the necessary asset(s) and actor(s) to enable the delivery of the goals.

Actors utilise assets to complete their goals, e.g., the IT technician's goal is to repair a printer and the corresponding asset is printer. In this example, the *IT technician* (actor) is not the risk owner of the *printer* (asset) and it requires another actor to make the *printer* available to the *IT technician*. The *Sales department* (actor) owns the printer and their goal is *to print the clients' invoices*; the IT technician depends on the Sales department to provide access to their printer for the IT technician to repair the printer and for the Sales department to print the clients' invoices, and both fulfil their goal.

Each goal could be restricted by none, one, or more than one constraints, while the asset that is available to the delivery of the goal could be subject to one or more constraints that may restrict the goal. Following the above example, the organisation's policy states that "The IT manager should authorise any changes or repair to electronic assets"; the IT technician's goal is now restricted by the organisation's policy and therefore, it cannot deliver its goal without the satisfaction of the proposed constraint, which is the approval of the IT manager.

Output

(i) list of goals to be fulfilled by actors
(ii) list of assets required for delivery of goals
(iii) list of constraints restricting goals

Normative references

(i) clause 5.1

4.4 Technical Viewpoint

Information security is the preservation of confidentiality, integrity, and availability of information assets. It depends upon forecasting of events through methodological and planned approaches such as information security risk management to estimate and direct information system through the current and future information incidents. A critical part of forecasting is to comprehend the flow of information and assessment of future incidents to information. The Technical Viewpoint offers a systematic information security risk management to forecast risks to the organisation and opportunities for the ISMS to achieve its intended outcome(s).

The Technical Viewpoint is a collection of seven interrelated views to assess the information outputs from the Operational Viewpoint and addressing the strategic needs of the organisation. Figure 4.13 illustrates an outline of the Technical Viewpoint modelled using INFORMS modelling language to demonstrate the interrelation of the views. The models relevant to the Operational Viewpoint are shown in opaque.

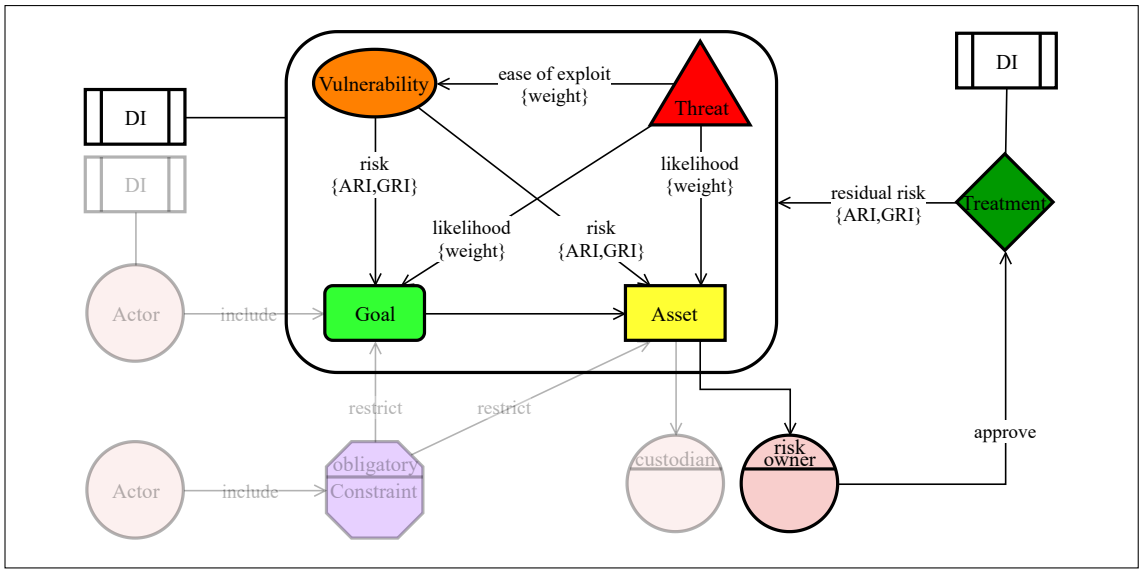


Figure 4.13: Outline of a Technical Viewpoint

The implementation of views in the Technical Viewpoint requires a blend of interested parties with core business background and information security expertise to facilitate the correct assessment and treatment of information security risk. The views together manage all the aspects of the information security risk, applied to the organisation's functions and processes. An activity diagram shown in Figure 4.14 demonstrates the proposed views and procedures to manage information security risk adopted by ISO/IEC 27005 [125].

The following describes the core processes involved in the Technical Viewpoint in managing information security risk:

Risk assessment is the overall process to materialise risks, including:

- Risk identification: a process to identify and recognise risks and their sources for the cause of a potential loss; it provides an understanding of how, where, and why a particular loss occurs. The Identification of Threats and Identification of Vulnerabilities views provide activities to identify threats' likelihood and ease of exploit as core inputs in the assessment of information security risks.
- Risk analysis: a process to study the consequences of risks to the organisation's assets and goals via Assessment of Impacts View and to establish the level of risks in the Risk Determination View.
- Risk evaluation: a process in the Risk Evaluation View to compare the levels of risk with risk criteria to determine whether the significance of risk is acceptable.

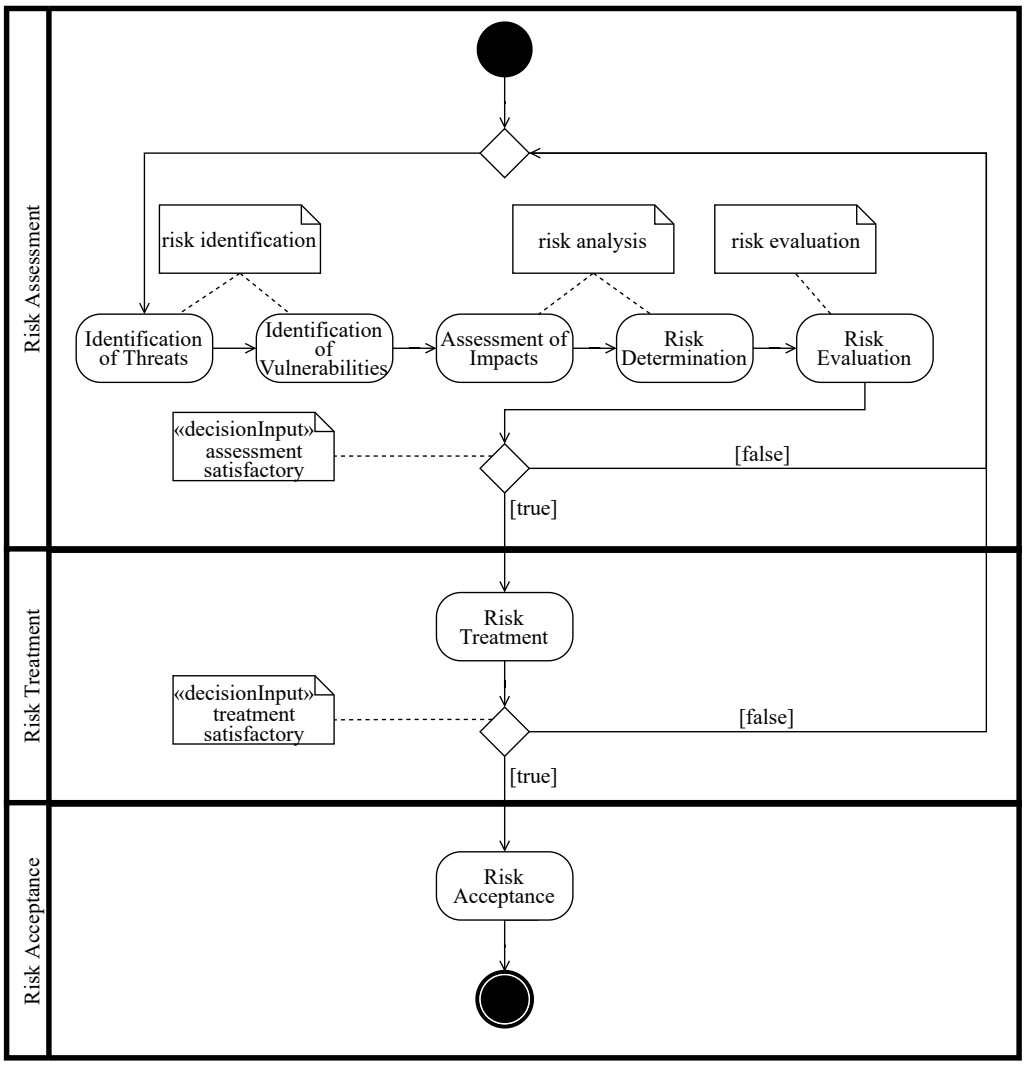


Figure 4.14: Activity diagram of information security risk management

Risk treatment is a process in the Risk Treatment View to modify risk by encompassing a plan to reduce, retain, avoid, or share the risk.

Risk acceptance is the final process in managing the information security risk to determine whether the organisation should accept and take a particular risk through reasoned judgement in the Risk Acceptance View.

4.4.1 Identification of Threats

This view models the threats and their likelihood of occurrence. The likelihood refers to the frequency of an incident scenario and the severity of an attack; it is a critical key indicator in the selection of an appropriate treatment plan. An activity diagram shown in Figure 4.15 demonstrates the processes involved in the Identification of Threats View.

Input

(i) output from Goal Delivery View

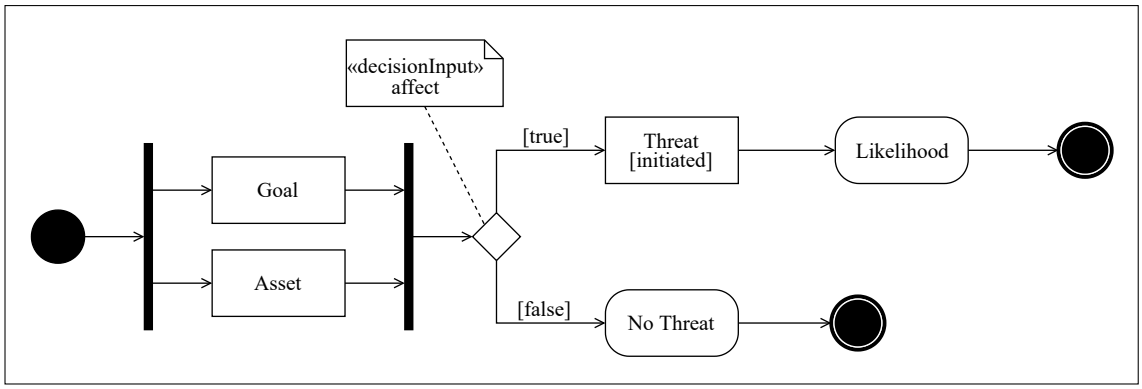


Figure 4.15: Activity diagram of Identification of Threats View

(ii) output from Asset Management View

(iii) list of known threats, e.g., threat catalogues

(iv) information on threats obtained from incident reviewing, risk owners, actors and other sources

Activity

In the context of information security, the concept of attack is a conventional definition of the threat that used interchangeably; however, the threat describes the source of the attack.

ISO/IEC 27000 [120] defines threat as a "potential cause of an unwanted incident, which may result in harm to a system or organization". Similarly, National Institute of Standards and Technology (NIST) [126] defines threat as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service".

The two definitions together emphasise important characteristics of threat, while both vary in depth of details. Both definitions agree that threat is a potential source of harm or impact, on assets and goals. Assets and actors' goals are sources of interest for threats, and organisations have a duty of care to identify threats to assets, goals, and information systems.

The harm could be accidental or deliberate from within or from outside the organisation. An information security threats could be classed into one or many high-level types and where appropriate individual threats within each type identified. The threat types could be introduced by:

- Physical damage, e.g., fire, pollution, dust.
- Natural disaster, e.g., flood, earthquakes.
- Loss of services, e.g., loss of power supply, failure of telecommunication.

– Compromise of information, e.g., disclosure, theft of media, eavesdropping.

– Infrastructure failure, e.g., equipment failure, software malfunction.

While the types of threat provide useful insight in determining the source of harm, the origin of the source should also be taken into consideration. The origin of threat may be of natural or human who could have particular motivations in causing possible harm to the organisation's assets and goals. The threats introduced by human origin may cause by personnel, hackers, computer criminals, terrorist, or industrial espionage. For instance, an internal actor with reduced awareness of information security could unintentionally introduce malicious code into an information system by responding to a Phishing [2] email or a disgruntled employee may cause a fraud for revenge. Similarly, an outsider such as a hacker could seek unauthorised access to the organisation for monetary gain.

The risk of insider threats compared to outsider threats is always an ongoing debate, a research of 300 companies of various sizes in the UK across several key sectors found that 58% of all security incidents posed by insider threats such as employees, ex-employees, and third parties [127]. The study showed that 87% of security threats caused by inadvertent errors of internal actors and 82% by their lack of awareness and understanding of IT security threats.

Each threat may affect more than one asset or goal, which could cause different consequences to each asset or goal depending on the risk scenario. Similarly, each type of threat has a different likelihood of occurrence to harm assets and goals; some threats could have a higher probability to happen with a possibility of lower impact and others could have more inferior to moderate rate of happening but cause significant impact on the organisation, e.g., social engineering versus flood.

The input to estimate the likelihood of a threat that may result into a successful exploits may be obtained from a number of sources including risk owners, users of assets or goals, facility management, information security specialist, support actors such as HR or legal department, national and international government agencies, industry research groups, threat catalogues and statistics from reliable sources, internal experiences, and past threat assessment. A comprehensive list of common threats to information security is provided in Appendix A.

The likelihood of each incident scenario should be systematically assessed using qualitative, quantitative, or other analysis techniques to establish how often a threat occurs. Table 4.3 defines levels of likelihood in semi-quantitative and qualitative methods. The provided values and definitions from this table act as guidelines for

[2] cybercrime in which a target is contacted by email or other communication channels by an attacker posing as a legitimate entity to lure individuals into obtaining sensitive information.

INFORMS, similar scoring methods or definitions could be adopted to meet the requirements of an organisation. Additionally, existing controls need to be considered when establishing the likelihood of threats.

Table 4.3: Likelihood level definitions

Semi-Quantitative values	**Qualitative values**	**Description**
1	Very Low	Rare
2	Low	Annual
3	Medium	Monthly
4	High	Weekly

Output

(i) list of threats harming each asset and goal

(ii) level of likelihood of incident scenarios

Normative references

(i) clause 6.1

(ii) clause 6.1.2

(iii) clause 8.1

4.4.2 Identification of Vulnerabilities

A vulnerability without a corresponding threat is not considered as harm since there is no trigger to exploit the vulnerability and does not require a treatment plan. The absent of exploit is not permanent and the organisation should be proactive in regular monitoring and assessment of the vulnerabilities to identify any evidence of exploit or changes to the vulnerability.

An activity diagram shown in Figure 4.16 demonstrates the processes involved in the Identification of Vulnerabilities View.

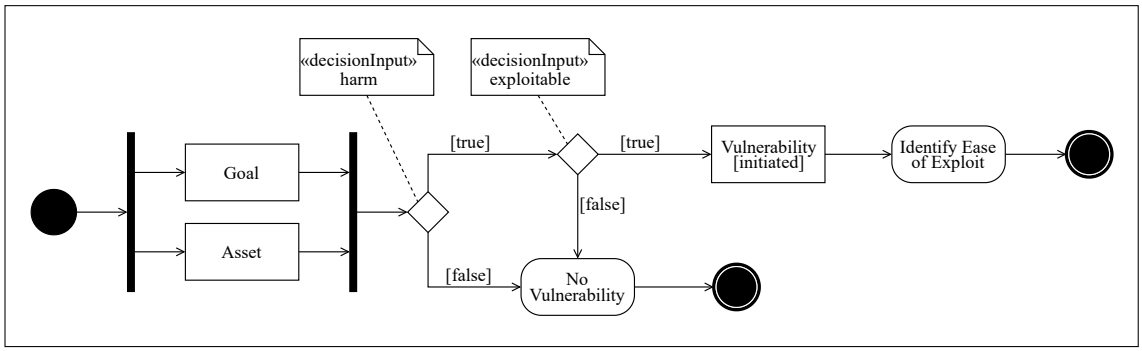


Figure 4.16: Activity diagram of Identification of Vulnerabilities View

Input

(i) output from Goal Delivery View

(ii) output from Asset Management View

(iii) output from Identification of Threats View

(iv) list of known vulnerabilities, e.g., vulnerability catalogues

Activity

The existence of vulnerability is not limited to information assets or goals, and vulnerabilities could be discovered in the processes and procedures, information system configurations and dependence on external actors.

Vulnerabilities could exist in the properties of the asset and how those properties configured. Similarly, the intention of use may change in the time than the initial purpose of the asset. Therefore, the description of goals and their dependency on assets or other goals should be regularly assessed to identify any new or gap in the vulnerabilities. It is vital that the organisation is aware of the rate of the exploitability of vulnerabilities and periodically review each and consider the severity of the vulnerability in terms of its exploitability.

The ease of exploitation by the threats to cause adverse consequences should be systematically assessed using qualitative, quantitative, or other analysis techniques. Table 4.4 defines levels of exploitability in semi-quantitative and qualitative methods. Again, the provided values and definitions from this table act as guidelines for INFORMS, similar scoring methods or definitions could be adopted to meet the requirements of an organisation. Additionally, existing controls need to be considered when establishing the likelihood of threats.

Table 4.4: Ease of exploit level definitions

Semi-Quantitative values	**Qualitative values**	**Description**
1	Very Low	Nearly impossible to exploit
2	Low	Difficult to exploit, requires high level knowledge of asset
3	Medium	Can be exploited with moderate knowledge of asset
4	High	Can be easily exploited by any one

Output

(i) list of vulnerabilities affecting each asset and goal

(ii) level of ease of exploit to each vulnerability

Normative references

(i) clause 6.1

(ii) clause 6.1.2

(iii) clause 8.1

4.4.3 Assessment of Impacts

A key part of the information security risk management is the assessment of the overall consequences that could happen from a possible or actual information security incidents, taking into account the impact of an information security incident on assets and goals of the organisation. An activity diagram shown in Figure 4.17 demonstrates the processes involved in the Assessment of Impacts View.

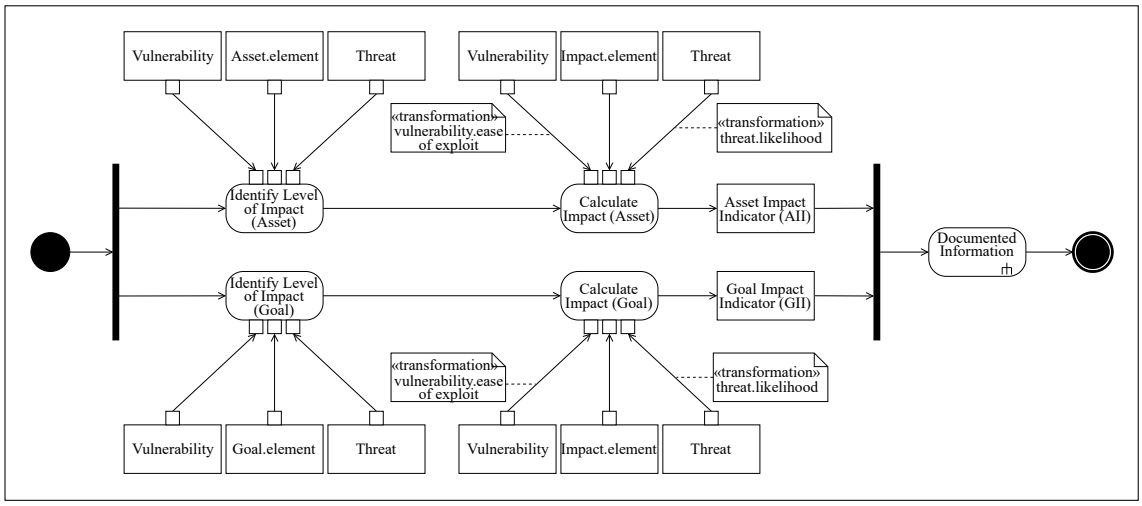


Figure 4.17: Activity diagram of Assessment of Impacts View

Input

(i) output from Goal Delivery View

(ii) output from Asset Management View

(iii) output from Identification of Threats View

(iv) output from Identification of Vulnerabilities View

Activity

INFORMS recognises asset and goal as the two domains for the assessment of consequences in information security risk; such an approach provides a comprehensive overview of consequences and an opportunity to analyse the disruption of operational functions that otherwise is not available by just considering the impact on assets. Both domains shall be analysed to enable a valid assessment of impacts.

After identifying the levels of threats' likelihood and ease of exploitation of vulnerabilities on assets and goals under review, values should be assigned to assets and goals while assessing the consequences.

Asset valuation begins with the classification of assets according to their criticality, in terms of the importance of assets to fulfilling the goals and strategic objectives

Table 4.5: Level definitions of the impacts on elements of asset

Element	Low	Medium	High
Confidentiality	Information can be disclosed to any individual, entity, or process	Information is not public and available to a group of authorised individuals, entities and processes	Information can only be disclosed to a privileged group of authorised individuals, entities and processes
Integrity	Information can be modified by all individuals, entities and processes	Information can be modified by a set of authorised individuals, entities and processes	Information can only be modified by the owner or a privileged group of authorised individuals, entities and processes
Availability	No requirement to have continuous access to information	Short periods of information unavailability are tolerable but normally authorised individuals, entities and processes require access	Information must be accessible to authorised individuals, entities and processes at all times

of the organisation. The impact on asset is based on the three fundamental elements of information security, which are confidentiality, integrity, and availability. Goal valuation is determined using the measures of business consequences of loss or compromise of the asset, such as the potential adverse business or legal consequences from the disclosure, or nonfulfillment of a goal.

The assessment of impacts on both domains achieve by considering Asset Impact Indicator (AII) and Goal Impact Indicator (GII); a semi-quantitative assessment to represent the level of impact on a particular asset and goal. A detailed explanation of both and the assessments of their elements are given below.

Asset Impact Indicator (AII) represents an aggregate score made up of three elements to establish the overall level of impact on an asset. The elements included in the determination of AII are listed below. In addition, Table 4.5 denotes the levels of impact on each element as low, medium, or high with their descriptive definitions.

- Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity: property of accuracy and completeness.
- Availability: property of being accessible and usable by an authorised entity.

A series of steps proposed to establish an Asset Impact Indicator for each asset in the organisation, including four steps as follow:

1. Identify the level of impact on each element of assets as low, medium, or high;

2. Calculate the value of impact on each element of assets by using the likelihood of the Threat (T), ease of exploitability of the Vulnerability (V), and the level of Impact (I) on a particular element of asset matched in a matrix such as that shown in Table 4.7 to identify the relevant measure of impact on a scale of 1 to 9. The formula to calculate the value of impact on elements is as below;

   Element [1-9]= T + V + I (element) [low-medium-high]

3. Apply the formula in step two to all three elements of assets. The result of this step should provide values for all elements similar to listed below; and

   Confidentiality [1-9] = T + V + I (confidentiality)
   Integrity [1-9] = T + V + I (integrity)
   Availability [1-9] = T + V + I (availability)

4. All three elements calculated in step three are represented in a nomenclature (aggregate score) for expressing Asset Impact Indicator, as shown below.

   Asset Impact Indicator = {confidentiality [1-9], integrity [1-9], availability [1-9]}

Here is an example to demonstrate the calculation of Asset Impact Indicator for an asset in a real-world scenario:
If the level of the threat's likelihood is *3 - Medium*, the ease of exploitability of the vulnerability is *4 - High*, and the impact on the: confidentiality is *Low*, integrity is *Low*, and the availability is *High*. The calculations and presentation of AII are listed below.

Confidentiality (6) = 3 + 4 + Low
Integrity (6) = 3 + 4 + Low
Availability (8) = 3 + 4 + High
$\Longrightarrow$ Asset Impact Indicator (AII) {6,6,8}

Goal Impact Indicator (GII) represents an aggregate score made up of seven elements to establish the overall level of impact on a goal. The elements included in the determination of GII are listed below. Similar to the AII, Table 4.6 denotes the levels of impact on each element of a goal as low, medium, or high with their descriptive definitions.

- Business: disruption of business activities.
- Financial: financial losses.
- Legal: inability to fulfil legal, regulatory, and contractual obligations.

– Physical: danger to the physical environment of personnel and user safety. physical refers to people, data, equipment, systems, facilities, company assets, site design and layout, environmental components [128].
– Privacy: breach associated with personal information.
– Social: adverse effects on the social fabric of the surrounding community.
– Technical: interruption of technical capability.

Table 4.6: Level definitions of the impacts on elements of goal

Element	**Low**	**Medium**	**High**
Business	Business operation can continue, none or limited inconvenience	Business operation can continue, but a major impact to volume of work is present	Business operation stops, catastrophic impact to volume of work is present
Financial	Does not exceed 0.1% of revenue	Greater than 0.1% but less than or equal to 1% of revenue	Exceeds 1% of revenue
Legal	Infringement or legal action is none or limited	Infringement or legal action is major and likely to happen	Infringement is catastrophic and legal action will happen
Physical	Physical harm is none or limited, would not cause any disruption	Physical harm is major, would lead to serious disruption	Physical harm is catastrophic, would lead to failure disruption
Privacy	Impact on privacy is none or limited, no PII records exposed	Impact on privacy is major, five or fewer PII records exposed	Impact on privacy is catastrophic, more than five PII records exposed
Social	Impact on the surrounding community is none or limited.	Impact on the surrounding community is major.	Impact on the surrounding community is catastrophic.
Technical	None or limited impact on the service, would not cause any disruption	Major impact on the service, would lead to serious disruption	Catastrophic impact on the service, would lead to failure disruption

A series of steps proposed to establish a Goal Impact Indicator for each goal in the organisation, including four steps as follow:

1. Identify the level of impact on each element of goals as low, medium, or high;
2. Calculate the value of impact on each element of goals by using the likelihood of the Threat (T), ease of exploitability of the Vulnerability (V), and the level of Impact (I) on a particular element of goal matched in a matrix such as that shown in Table 4.7 to identify the relevant measure of impact on a scale of 1 to 9. The level of likelihood and the level of ease of exploitability shall be the

same value for both asset and goal in a particular scenario. The formula to calculate the value of impact on elements is as below;

Element [1-9]= T + V + I (element) [low-medium-high]

3. Apply the formula in step two to all seven elements of goals. The result of this step should provide values for all elements similar to listed below; and

   Business [1-9] = T + V + I (business)
   Financial [1-9] = T + V + I (financial)
   Legal [1-9] = T + V + I (legal)
   Physical [1-9] = T + V + I (physical)
   Privacy [1-9] = T + V + I (privacy)
   Social [1-9] = T + V + I (social)
   Technical [1-9] = T + V + I (technical)

4. All seven elements calculated in step three are represented in a nomenclature (aggregate score) for expressing Goal Impact Indicator, as shown below.

   Goal Impact Indicator = {business [1-9], financial [1-9], legal [1-9], physical [1-9], privacy [1-9], social [1-9], technical [1-9]}

Here is an example to demonstrate the calculation of Goal Impact Indicator for a goal in a real-world example, using the same values for the threat's likelihood and the ease of exploitability of the vulnerability provided in the aforementioned scenario:
If the level of the threat's likelihood is *3 - Medium*, the ease of exploitability of the vulnerability is *4 - High*, and the impact on the: business is *High*, financial is *High*, legal is *Low*, physical is *Medium*, Privacy is *Medium*, Social is *High*, Technical is *Low*. The calculations and presentation of AII are listed below.

Business (8) = 3 + 4 + High
Financial (8) = 3 + 4 + High
Legal (6) = 3 + 4 + Low
Physical (7) = 3 + 4 + Medium
Privacy (7) = 3 + 4 + Medium
Social (8) = 3 + 4 + High
Technical (6) = 3 + 4 + Low
$\Longrightarrow$ Goal Impact Indicator (GII) {8,8,6,7,7,8,6}

The values in the matrix are placed in a structured manner. The size of the matrix in terms of the number of threat levels, vulnerability levels and the levels of

impact on elements, can be adjusted to the needs of the organisation. Additional columns and rows will necessitate additional risk measures.

Other methods of assessment, such as assigning a monetary value, cost-benefits, concerns of stakeholders, and other quantitative variables may provide more information for decision making and accuracy.

Output

(i) list of AII for all assets

(ii) list of GII for all goals

Normative references

(i) Clause 6.1.2

(ii) Clause 8.1

4.4.4 Risk Determination

An organisation shall determine risk as part of a formal analysis of risk. INFORMS proposes a semi-quantitative risk analysis by assigning numeric values to all facets of the risk analysis process, including the likelihood of threats, ease of exploiting vulnerabilities and impacts on assets and goals. Equations used to determine total and residual risks.

Table 4.7: Impact matrix

Threat	**Vulnerability**	**Impact**		
		Low	**Medium**	**High**
(1) Very Low	(1) Very Low	1	2	3
	(2) Low	2	3	4
	(3) Medium	3	4	5
	(4) High	4	5	6
(2) Low	(1) Very Low	2	3	4
	(2) Low	3	4	5
	(3) Medium	4	5	6
	(4) High	5	6	7
(3) Medium	(1) Very Low	3	4	5
	(2) Low	4	5	6
	(3) Medium	5	6	7
	(4) High	6	7	8
(4) High	(1) Very Low	4	5	6
	(2) Low	5	6	7
	(3) Medium	6	7	8
	(4) High	7	8	9

An activity diagram shown in Figure 4.18 demonstrates the processes involved in the Risk Determination View.

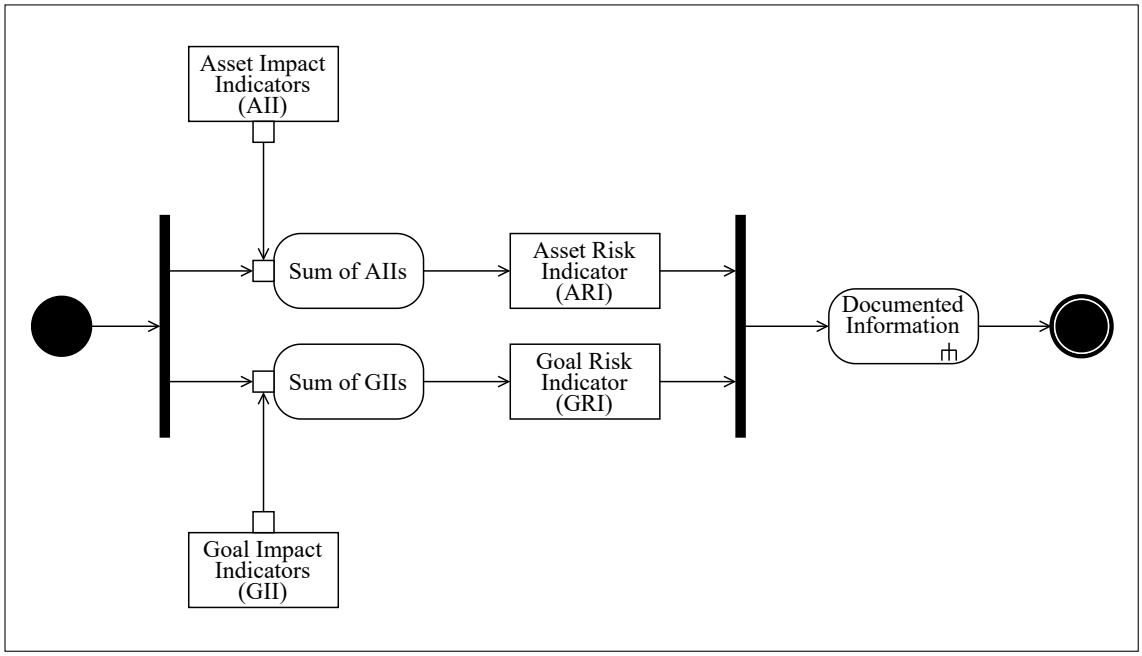


Figure 4.18: Activity diagram of Risk Determination View

Input

(i) output from Assessment of Impacts View

Activity

Similar to the assessment of impacts on both assets and goals, the same approach identified in determining information risk. Both domains shall be analysed to enable a valid determination of risks. The determination of risks on both domains achieves by considering Asset Risk Indicator (ARI) and Goal Risk Indicator (GRI); a semi-quantitative assessment technique to represent the level of risk on assets and goals. A detailed explanation of both areas and method of determining risk on both are given below.

Asset Risk Indicator (ARI) represents the overall level of risk to an asset. It is a quantitative value based on assessed consequences to the asset. The formula to determine the value of risk on an asset is as below.

$$\text{Asset Risk Indicator} = \sum \text{Asset Impact Indicator}$$

Following the previously mentioned scenario in the Impact Assessment View, here is a demonstration of determining the risk on the asset by calculating Asset Risk Indicator:

$$\text{Asset Impact Indicator (AII) } \{6,6,8\} \longmapsto \sum 6,6,8$$
$$\implies \text{Asset Risk Indicator (ARI) } \{20\}$$

Goal Risk Indicator (GRI) represents the overall level of risk to a goal. It is a quantitative value based on assessed consequences to the goal. The formula to determine the value of risk on a goal is as below.

$$\text{Goal Risk Indicator} = \sum \text{Goal Impact Indicator}$$

Following the above scenario, here is a demonstration of determining the risk on the goal by calculating Goal Risk Indicator:

$$\text{Goal Impact Indicator (GII) } \{8,8,6,7,7,8,6\} \longmapsto \sum 8,8,6,7,7,8,6$$
$$\Longrightarrow \text{Goal Risk Indicator (GRI) } \{50\}$$

Output

(i) list of ARI for all assets

(ii) list of GRI for all goals

Normative references

(i) Clause 6.1.2

(ii) Clause 8.2

4.4.5 Risk Evaluation

Organisations shall evaluate risks by comparing the estimated risks with the risk evaluation criteria defined based on the context of the organisation. An activity diagram shown in Figure 4.19 demonstrates the processes involved in the Risk Determination View.

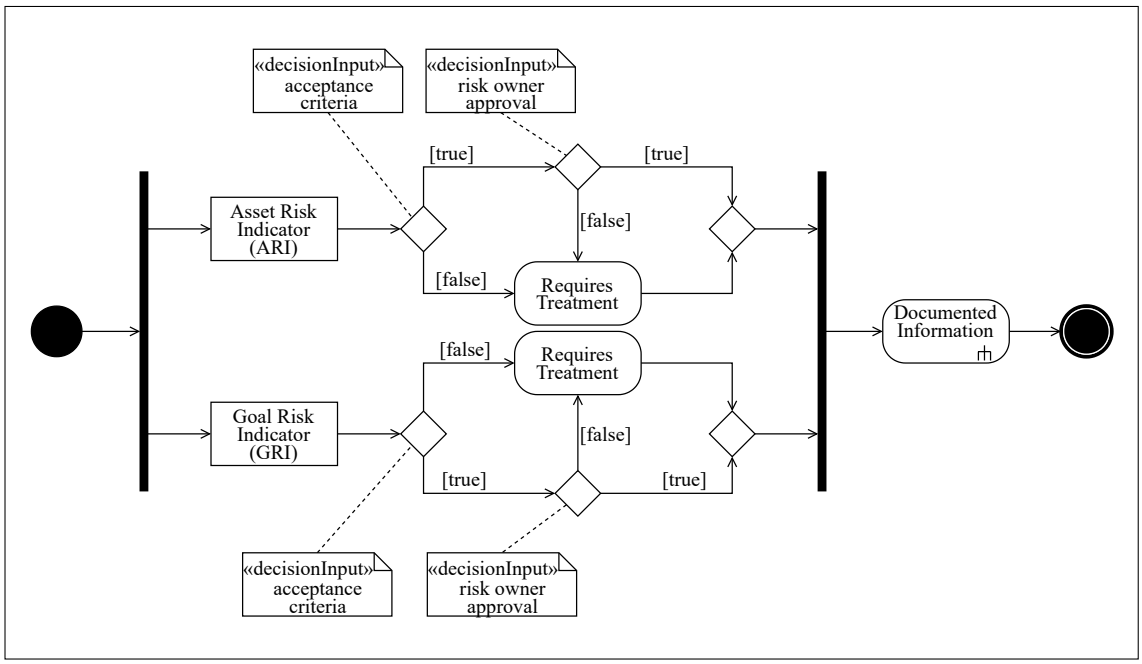


Figure 4.19: Activity diagram of Risk Evaluation View

Table 4.8: Evaluation criteria for Asset Risk Indicator

Semi-quantitative values	Qualitative values	Description
3-9	Very Low	Can be accepted without any treatment
10-15	Low	Risk owner must accept or reduce the risk
16-21	Medium	Action should be taken to reduce the risk. The top management may accept.
22-27	High	Action must be taken to reduce the risk

Input

(i) output from Risk Determination View

(ii) risk evaluation criteria

Activity

Risk evaluation criteria used to make decisions should be consistent with the context and objectives of the organisation. The nature of the decisions pertaining to risk evaluation criteria is usually decided when establishing the context of the organisation. These decisions should be revisited and updated as appropriate to reflect the current setting of the organisation, e.g., changes in the law and regulations.

Decisions related to the risk evaluation activity are mainly based on the acceptable level of risk while the likelihood and individual degree of impact to each element of asset or goal should be considered too. Aggregation of multiple low or medium risks may result in much higher overall risks which also needs to be taken into account when accepting the risk [125].

Table 4.8 defines the criteria for acceptance and evaluation of the Asset Risk Indicator in semi-quantitative and qualitative methods. The provided values and definitions from this table act as guidelines for INFORMS, similar scoring methods or definitions could be adopted to meet the requirements of an organisation. Additionally, existing controls need to be considered when evaluating risks.
Following the previously mentioned scenario in the Risk Determination View, here is the evaluation result for that particular Asset Risk Indicator based on the evaluation criteria provided in Table 4.8.

> Asset Risk Indicator (ARI) {20}
> $\Longrightarrow$ The risk value of 20 is within the category of 16-21 defined as Medium, meaning that "Action (treatment plan) should be taken to reduce the risk. The top management may accept."

Table 4.9 defines the criteria for acceptance and evaluation of the Goal Risk Indicator in semi-quantitative and qualitative methods.

Table 4.9: Evaluation criteria for Goal Risk Indicator

Semi-quantitative values	**Qualitative values**	**Description**
7-15	Very Low	Can be accepted without any treatment
16-31	Low	Risk owner must accept or reduce the risk
32-47	Medium	Action should be taken to reduce the risk. The top management may accept.
48-63	High	Action must be taken to reduce the risk

Following the above scenario, here is the evaluation result for that particular Goal Risk Indicator based on the evaluation criteria provided in Table 4.9.

> Goal Risk Indicator (ARI) {50}
> $\Longrightarrow$ The risk value of 50 is within the category of 48-63 defined as High, meaning that "Action (treatment plan) must be taken to reduce the risk."

As pointed out in the evaluation of the risks in the above examples, there is also a difference between the evaluation category of ARI and GRI. The ARI is categorised as Medium during the evaluation while in the same scenario, GRI is categorised as High. Although the difference between them is marginal, the evaluation of risk to asset and goal may produce a different result; both domains assessed using the same level of likelihood, ease of exploit, and the corresponding correlation in allocating the evaluation categories. This indicates the particular risk scenario has a higher consequence to the goal than the asset if the risk materialised.

Output

(i) list of ARI and GRI prioritised according to risk evaluation criteria concerning the incident scenarios

Normative references

(i) Clause 6.1.2

(ii) Clause 8.2

4.4.6 Risk Treatment

Organisations should treat information security risks using appropriate options to reduce, retain, avoid or share the risks based on the outcome of the risk assessment. A detailed description of each option is discussed in Section 3.3.9. An activity diagram shown in Figure 4.20 demonstrates the processes involved in the Risk Treatment View.

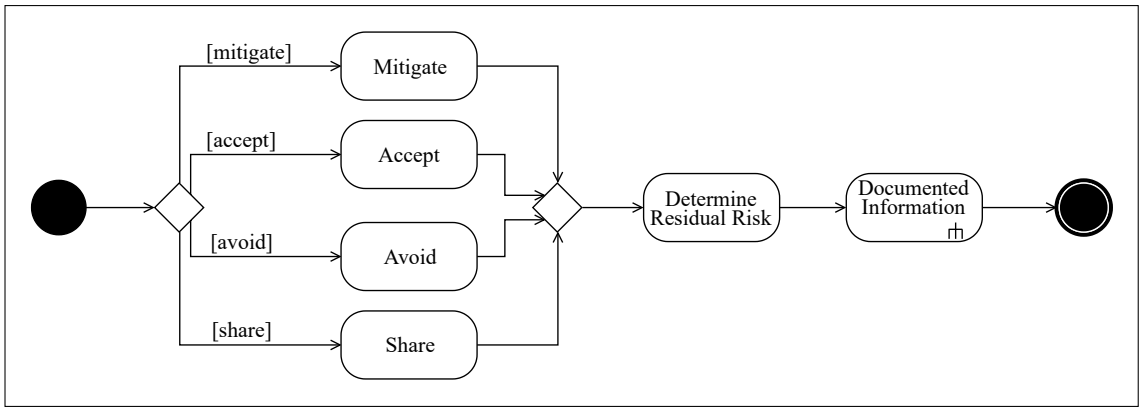


Figure 4.20: Activity diagram of Risk Treatment View

Input

(i) output from Constraint Specification View

(ii) output from Assessment of Impacts View

(iii) output from Risk Determination View

(iv) output from Risk Evaluation View

Activity

The effectiveness of the risk treatment depends on the results of the risk assessment. The standard specifies that the selection and implementation of treatment controls need to be risk-based. The application of a risk management process, such as one proposed in the Technical Viewpoint, can satisfy this requirement. There are many approaches by which the process can successfully implement in an organisation. The organisation should use whatever method best suits their circumstances for each specific application of the process.

Some risk treatments can effectively address more than one risk, e.g., information security training and awareness. A risk treatment plan should identify the priority order in which individual risk treatments should implement and their time frames. Priorities can establish using various techniques, including risk ranking and cost-benefit analysis. It is the organisation's responsibility to decide the balance between the costs of implementing controls and the budget assignment.

The documented information of the ISMS should provide evidence that treatment controls are selected based on the consideration of risk to information, and such decisions align with the information security policy and objectives. A cyclical process of the risk treatment as provided by ISO/IEC 27005 [125] include:

- assessing a risk treatment;
- deciding whether residual risk levels meet the risk acceptance criteria;
- introducing a new treatment plan if risk levels are not acceptable; and
- assessing the effectiveness of the new risk treatment.

The four options for risk treatment are not mutually exclusive, and a combination of options such as reducing the likelihood of risks, reducing their consequences, and sharing or retaining any residual risks can benefit the organisation. Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementing these options, and the expected benefits from these options. Additionally, all constraints and organisational context should be taken into account during the risk treatment since they provide information on legal and regulatory requirements with which the organisation needs to comply.

This selection of risk treatment options should also take account of cost and time frame for implementation of controls, as well as the impact on the elements of the goal. The adverse consequences of risks should be made as low as reasonably practicable, and consideration should be given to rare but severe risks. Further consideration should be given to specialised skills that may be needed to define and implement new controls or modify existing ones [125].

As for the selected controls, the establishment and documentation of the procedures should have a reference to the person responsible for the actual piece of documentation [124]; documentation is essential for the traceability and reproducibility of results and procedures.

Once the risk treatment plan has been defined, residual risks need to be determined. The residual risk or alternatively known as retained risk refers to the potential for reoccurrence of an adverse event after adjusting risk treatment [129]. The determination of the residual risk involves a re-iteration of the risk assessment by taking into account the expected effects of the proposed risk treatment. If the reassessed risk still not meet the organisation's risk acceptance criteria, then a further iteration of risk treatment may be necessary before proceeding to risk acceptance.

It is possible that the risk treatment not immediately lead to an acceptable level of residual risk. In this situation, another iteration of risk assessment with changed context parameters, e.g., change of assessment method may help.

The identification of existing controls may determine that existing controls exceed current needs, in terms of cost comparisons, including maintenance. If removing redundant or unnecessary controls is considered, it should be taken into account that controls may influence each other, eliminating redundant controls might reduce the overall security in place.

Output

(i) list of risk treatment plans for each identified risk scenario, subject to the acceptance decision of the relevant risk owner

(ii) list of residual risks

Normative references

(i) clause 6.1.3

(ii) clause 8.3

4.4.7 Risk Acceptance

The risk acceptance is a process to explicitly accept the residual risks based on an informed decision by the risk owners. An activity diagram shown in Figure 4.21 demonstrates the processes involved in the Risk Acceptance View.

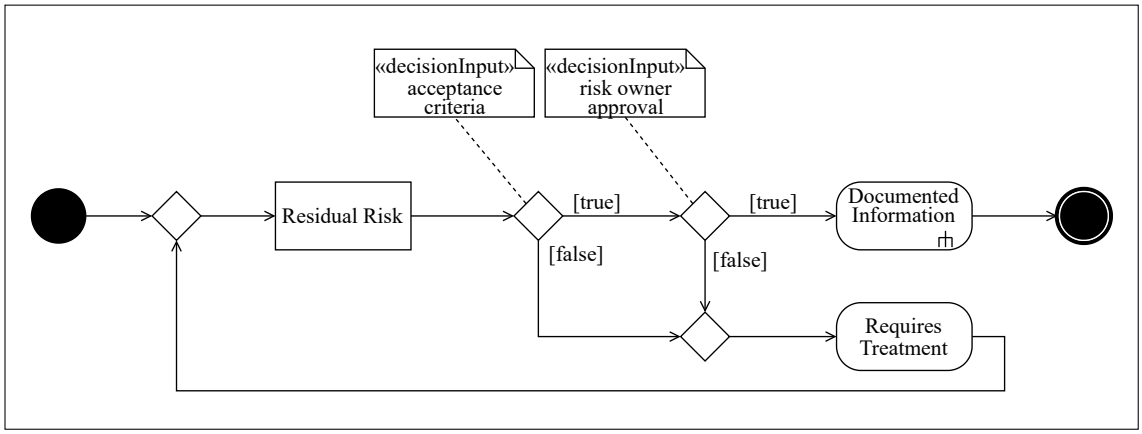


Figure 4.21: Activity diagram of Risk Acceptance View

Input

(i) output from the Assessment of Impacts View

(ii) output from the Risk Evaluation

(iii) output from the Risk Treatment View

Activity

Most risks are satisfied through the implementation of appropriate treatment plans, while some residual risks exist that has a reasonable level of potential impacts on the organisation. The decision to accept the risks and responsibilities for the decision should be made and formally recorded by the organisation, this becomes additionally important in a situation where the implementation of treatment controls are omitted or postponed, e.g., due to cost.

Risks may be accepted if it is evaluated that the risk meets the acceptance criteria, i.e., the level of risk is low or negligible. Additionally, a risk may be accepted if the cost of a treatment control is uneconomic; judgement needs to be exercised as to whether the cost of a treatment plan is commercially justifiable. For example, the expense of treating the risk exceeds beyond the cost of loss due to exploitation.

The selection and implementation of the risk treatment plan should be reviewed to ensure the risks meet the risk acceptance criteria. The risk owner has the re-

sponsibility to review and approve risk treatment plans and residual risks.

Risk owners should consider that some residual risks may not meet risk acceptance criteria because the criteria being applied do not take into account prevailing circumstances, e.g., the cost of risk modification is too high.

Output

(i) list of accepted risks with justification for inclusion and exclusion

Normative references

(i) clause 6.1.2

(ii) Clause 6.1.3

4.5 System Viewpoint

This viewpoint is a backbone of the INFORMS framework, it is about Who and What of the ISMS and refers to the high-level requirement of the standard. The System Viewpoint represents in two unrelated views that each depict organisational processes and their interaction with all other views in the framework, the views included are the Role Description View and Objectives Specification View.

The viewpoint is structurally positioned in the middle layer of the framework to act as a central point in the overall execution of the management system. As the title of the viewpoint suggests, the System Viewpoint is an abridged version of the Management System, which in this research is the information security management system.

While most views in the framework can produce and flow inputs to other management systems such as ISO 9001 or ISO/IEC 20000-1, the views in the System Viewpoints are intentionally segregated to produce outputs applicable for the use and needs of ISO/IEC 27001, i.e., the outputs from this viewpoint is only relevant and useful for the processes in the ISMS.

An outline of the System Viewpoint modelled using INFORMS modelling language to demonstrate the interrelation of the views is presented in Figure 4.22. The models relevant to the Operational and Technical viewpoints are shown in opaque.

4.5.1 Roles Description

Top management shall define, assign, and communicate all roles and responsibilities relevant to the information security throughout the organisation.

Input

(i) output from the Leadership View

(ii) output from the Actor Description View

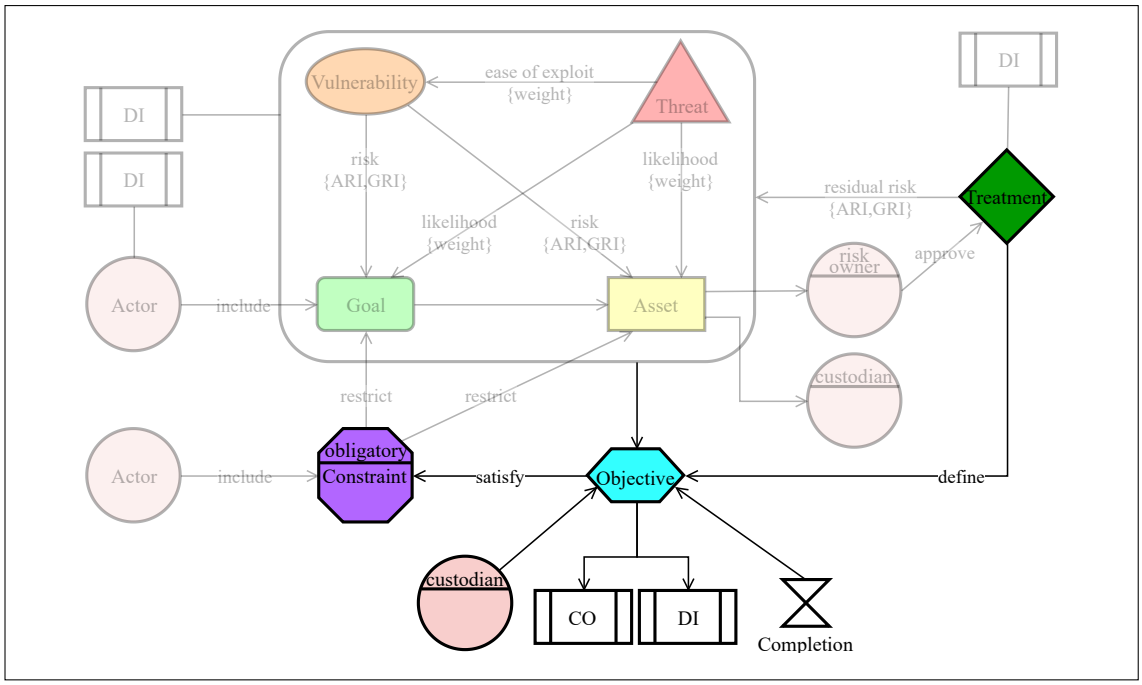


Figure 4.22: Outline of a System Viewpoint

Activity

The types of roles introduced and used by the INFORMS framework discussed in the Role concept in Section 3.3.6. The assigned responsibilities ensure that execution of the ISMS is in conformance with the requirements of the standard. Further, this enables the top management to receive a report of the performance and effectiveness of the ISMS.

Apart from the responsibilities specifically assigned relevant to information security, accountability towards information security should include within other roles, i.e., information security responsibilities can incorporate in the roles of information owners, process owners, risk owners, project managers, and information users.

Table 4.10 provides a list of views matched with their required roles; some views may need more than one role type to fulfil its processes.

Output

(i) list of actors with assigned responsibilities

Normative references

(i) clause 5.3

4.5.2 Objectives Specification

This view aims at specifying objectives of the ISMS; low-level directions prescribed on how to achieve the overall expectation of the information security as described in the Policy View.

Table 4.10: Views with assigned responsibility

View	Auditor	Analyst	Collector	Custodian	Risk owner
Awareness				+	
Communication				+	
Asset Management				+	+
Risk Treatment					+
Objectives Specification				+	
Monitoring & Measurement		+	+		
Internal Audit	+				

An activity diagram shown in Figure 4.23 demonstrates the processes involved in the Objectives Specification View.

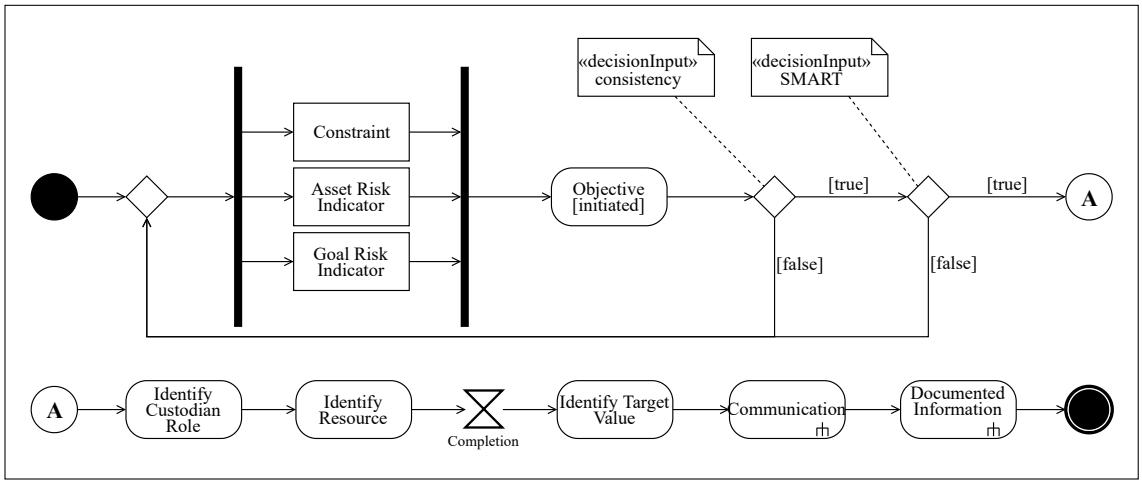


Figure 4.23: Activity diagram of Objectives Specification View

Input

(i) output from Scope View

(ii) output from Policy View

(iii) output from Actor Description View

(iv) output from Constraints Specification View

Activity

The directions on how to set objectives may come from the constraints introduced by the actors and internal and external issues that could affect the organisation's ability to achieve the intended outcomes of its information security management system. Organisations develop various policies or comply with laws relevant to their applicable industry, e.g., information security policy, GDPR. Consideration should

be given at specifying objectives to be consistent with such policies and laws.

The security policy identifies what to achieve, and the security objective responds on how to accomplish the security policy. Information security policy supports the organisation in achieving its objectives.

Each specified objective should be methodologically constructed to provide actions that either directly support the requirements of the standard or improve the overall effectiveness of the ISMS, i.e., objectives should be SMART. The concept of SMART [130] is an approach developed for setting objectives effectively and productively. Organisations could adopt other methods as their objective setting approach. The SMART is an acronym tied to five criteria, as indicated below.

Specific: explicit action on a specific area of improvement

Measurable: quantifiable feature as an indicator of progress

Achievable: realistically achieved on the right level

Relevant: appropriate to the (information security) goals of the organisation

Time-framed: indication of when the results should accomplish

The fulfilment of the objectives satisfies through the implementation of the treatment controls established in the Technical Viewpoint. Also, the satisfaction of the constraints should be demonstrated by proposing appropriate objectives and/or information security treatment.

All objectives should collectively provide tactical information on the current and/or desired relationships between the organisation's mission and the management processes related to information security. Such information support beyond the details of the information system operation by considering responsible role to oversight the satisfaction of the objectives, the necessary resources to implement the objectives, and completion date for meeting the requirements of the objectives. Additionally, the objectives should be communicated with the internal and external actors (where relevant) to ensure they are aware of their impacts on the implementation of the objectives.

The objectives shall be monitored and analysed at regular interval to measure their progress and contribution to the effectiveness of the ISMS. The achievement of each objective should be evaluated against appropriate target criteria to assess the result of the objectives. The criteria for the target should be achievable and realistic to enable the organisation to improve the ISMS continually; the necessary adjustment to the target or the objectives itself is considered when appropriate.

Output

(i) list of information security requirements from the actors

(ii) document summarising the objectives including organisational requirements

Normative references

(i) clause 5.2

(ii) clause 6.2

4.6 Standard Viewpoint

The previous viewpoints in the framework introduced to model the overall architecture of the ISMS; by contrast, the Standard Viewpoint models the analysis of the implemented architecture of the ISMS. It evaluates the overall effectiveness of the ISMS, i.e., acts as quality assurance and enhancement of the ISMS.

There are five views to constitute the Standard Viewpoint, on the whole, to ensure that the current structure of the ISMS conforms with the overall requirements of the standard. Figure 4.24 outlines of a Standard Viewpoint modelled using the INFORMS modelling language to demonstrate the interrelation of the views, the models relevant to all other viewpoints are shown in opaque.

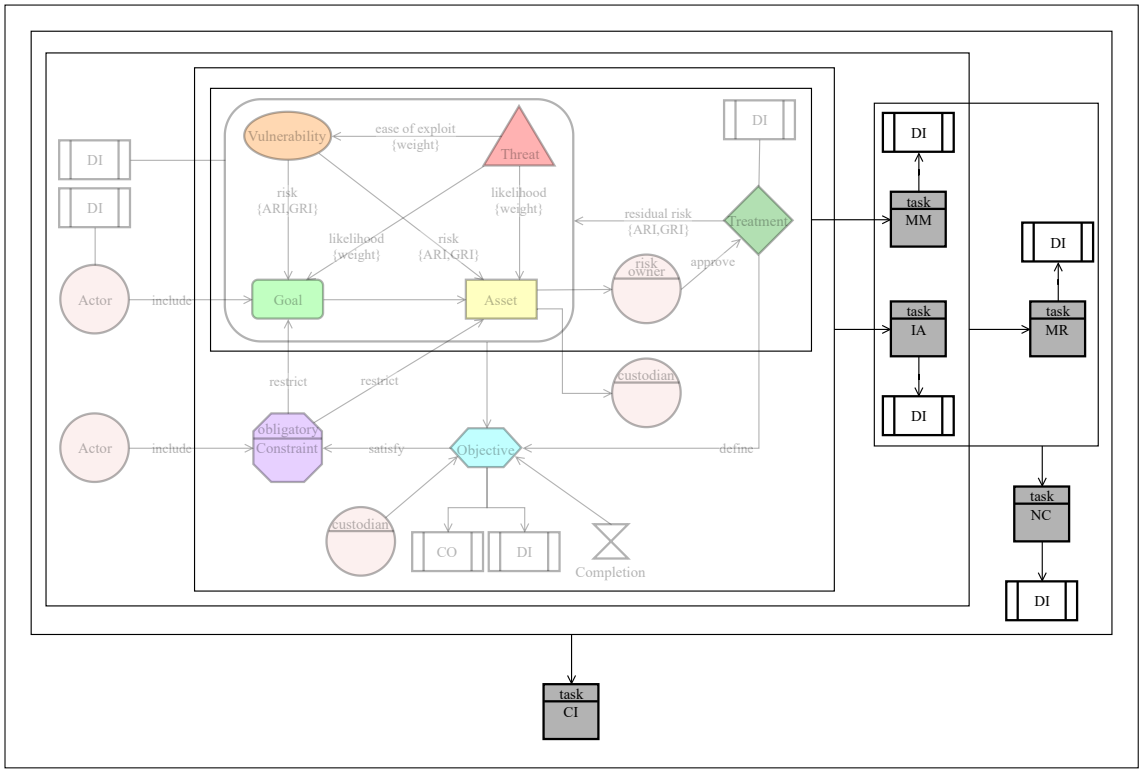


Figure 4.24: Outline of a Standard Viewpoint

4.6.1 Monitoring and Measurement

Organisations need to establish planned activities to monitor, measure, analyse, evaluate the ISMS and its effectiveness to ensure it meets the requirements of the standard as well as the organisation. Successful implementation of ISMS verifies by

continuous assessment of its performance. An activity diagram shown in Figure 4.25 demonstrates the processes involved in the Monitoring and Measurement View.

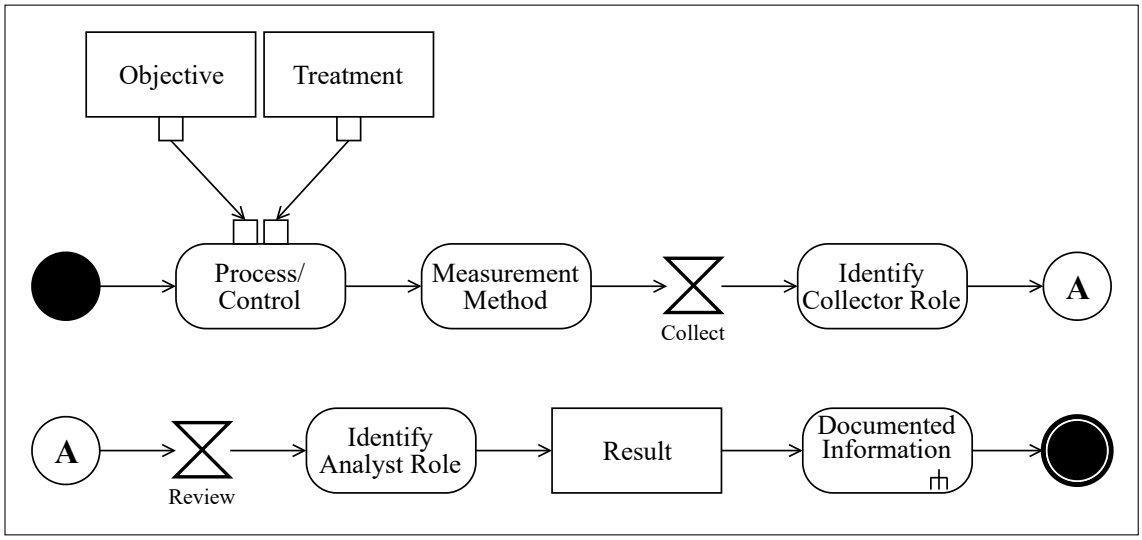


Figure 4.25: Activity diagram of Monitoring and Measurement View

Input

(i) output from Risk Treatment View

(ii) output from Objective Specification View

Activity

Monitoring observes the status of a process while measurement is an act to determine a value. Monitoring is achieved through planned measurement over some time, both activities enable the organisation to comprehend and determine if the intended outcomes of the ISMS are achieved by evaluating the result of monitoring and measurement.

The need for monitoring and measurement should be triggered at what information is required to monitor and measure. The information need is a high-level question or statement that directs the organisation in collecting the information required for evaluating the information security performance and ISMS effectiveness.

The monitoring activities produce data that can use to support the measurement; the two types of measures include performance measurement and effectiveness measurement. The former is a pre-defined activity with the planned result to establish the performance of the information security processes and controls, e.g., headcount. Effective measurement is an overall evaluation to indicate the pre-defined activities meet the information security objectives.

The organisation should establish methods for monitoring and measurement to provide comparable and reproducible results to be considered valid. The method should define suitable timeframes in which to monitor, measure, analyse and evaluate

the performance of the ISMS based on their information needs, such as constraints, organisation's strategic direction, information security policy and objectives, and the result of the risk treatment.

The interval (collect) indicates the frequency of the monitoring and measurement to be collected on the identified processes and controls, while the interval (review) shows the frequency of when the result of the monitoring and measurement should be reviewed. The activity requires two roles involved in collecting and reviewing monitoring and measurement processes and controls; both roles could be performed by one actor or more than one. Similarly, the use of automated methods and assisted application such as event analyser could be employed if applicable to deliver the monitoring and measuring activity.

The organisation can adjust its measurement timeframes as they change their goals and activities to address the updated information need. For example, if an organisation is switching from a private cloud provider to a public cloud provider, a change in frequency of collection of logs is required. Further, a change in the analysis and evaluation of the logs from the service provider should be updated to address the new requirements of the organisation.

Output

(i) methods to monitor, measure, analyse and evaluate
(ii) completion times for monitoring and review of each process
(iii) roles and responsibilities for monitoring and review of each process
(iv) documented evidence of monitoring and measurement results

Normative references

(i) Clause 9.1

4.6.2 Internal Audit

Conducting an internal audit is another method of assessment for the organisations to evaluate the conformity of the ISMS implementation against the requirements of the standard. It assures the top management on the suitability, adequacy and effective implementation of the ISMS. An activity diagram shown in Figure 4.26 demonstrates the processes involved in the Monitoring and Measurement View.

Input

(i) output from the result of the previous Internal Audit (if applicable)

Activity

The conduct of audit confirms whether the ISMS is effectively implemented and maintained as per requirements of the standard. Auditing is an activity that helps an organisation to gain insight to the operation of the ISMS by understanding whether

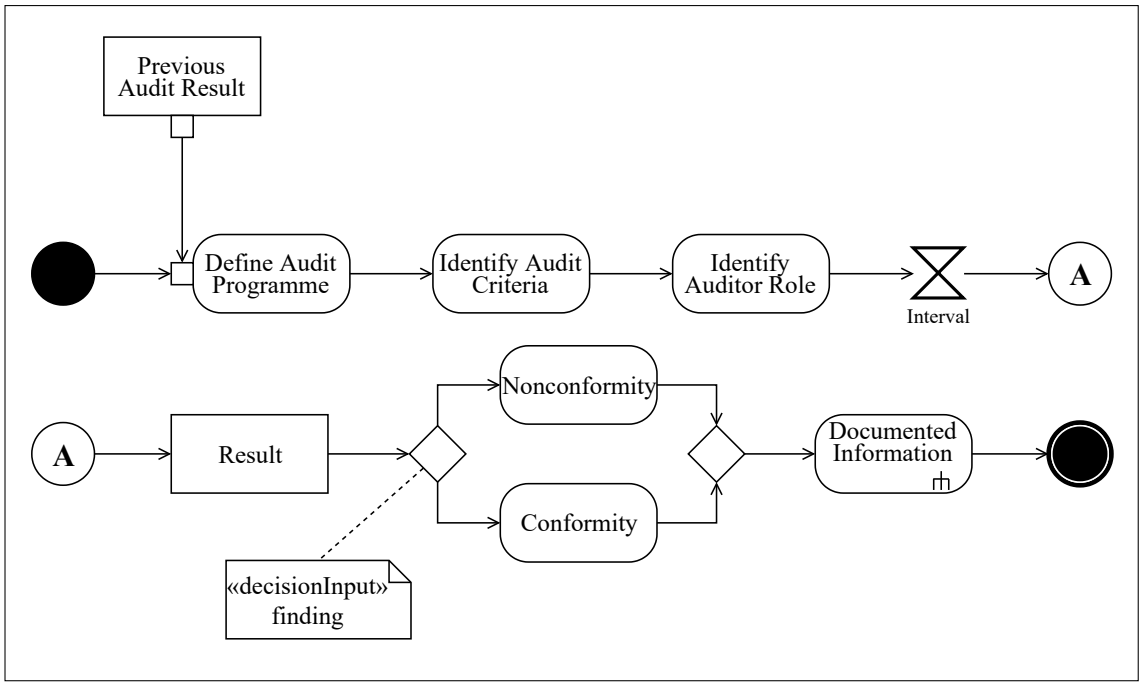


Figure 4.26: Activity diagram of Internal Audit View

the organisation conforms with its information security policy and objectives, the outcome of the risk treatment process, constraints, and documented information.

Each internal audit requires a programme to identify specific parameters of the audit, including a working plan of the audit, frequency, methods, and planning requirements. The audit programme should take into consideration the importance of the activities and processes in the organisation and the result of the previous internal audits.

The audit must be carried out against an identified audit scope and defined a set of audit criteria which the audit findings are evaluated against the criteria. The organisation should assign competent and independent auditor(s) to ensure the objectivity and the impartiality of the audit result. Internal audit should be carried out with integrity, due professional care, confidentiality, independence and evidence-based approach.

The result of the audit should be analysed and reported to relevant top management for consideration of the outcomes. The result of the audit could identify non-conformities, risks and opportunities for continual improvement. The former output is addressed according to the Nonconformities and Corrective Actions View, while, the latter is considered in the management of information security risks in the Technical Viewpoint.

Output

(i) evidence of audit programme

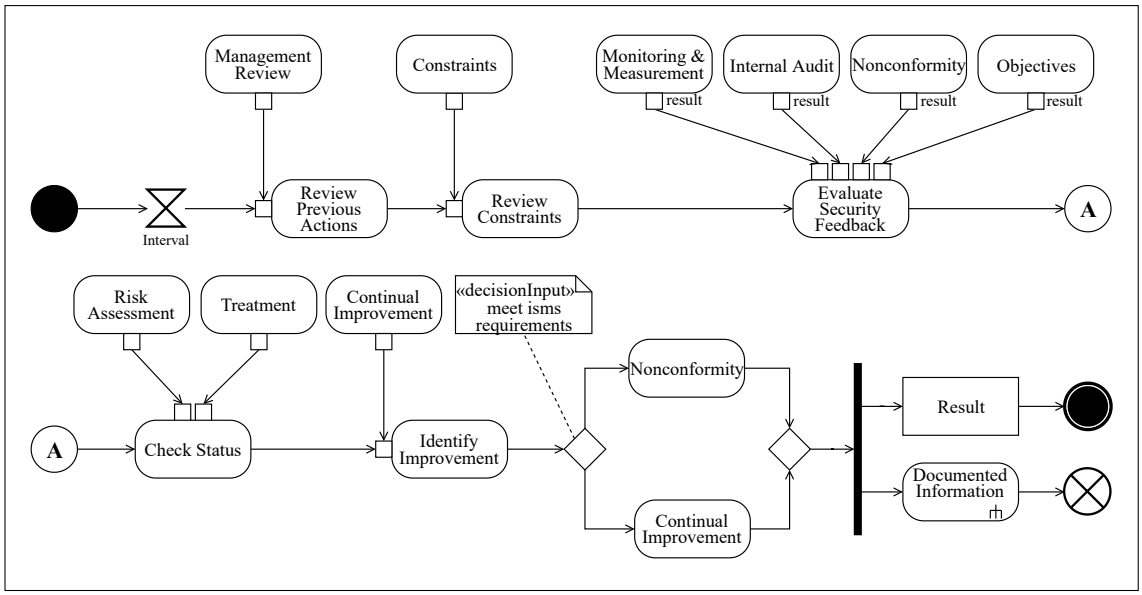


Figure 4.27: Activity diagram of Management Review View

(ii) evidence of a plan for each planned audit

(iii) roles and responsibilities for conducting the audit

(iv) completion times for each audit process

(v) evidence of audit results

Normative references

(i) Clause 9.2

4.6.3 Management Review

The process of a management review is another method of assessment to evaluate the performance of the ISMS. An activity diagram shown in Figure 4.27 demonstrates the processes involved in the Management Review View.

Input

(i) output from Constraint Specification View

(ii) output from Risk Assessment View

(iii) output from Objectives Specification View

(iv) output from Monitoring and Measurement View

(v) output from Internal Audit View

(vi) output from the result of the previous Management Review (if applicable)

(vii) output from Nonconformity and Corrective Actions View

Activity

ISMS is a live process that requires regular evaluation to ensure its suitability and effectiveness meets the requirements of the organisation as well as the standard. The top management has the overall responsibility for continual alignment of the

ISMS with the organisation's information security policy. It needs to ensure the processes and operations are effectively implemented to achieve the objectives of information security. The top management should review the result of the processes at planned intervals, at least once a year.

The agenda of the review meetings should include consideration of the following topics:

- Status of actions from previous management reviews.
- Changes to the constraints.
- Results of the monitoring and measurements.
- Results of internal audits.
- Status of information security objectives fulfilment.
- Result of nonconformities and corrective actions.
- Feedback from actors.
- Results of information security assessments.
- Status of information security risk treatment plan.

The outcome of a management review process should include decisions related to continual improvement, and any changes may require for the ISMS. The top management may consider changes to information security policy and objectives, changes to resources, risk acceptance criteria, any corrective actions required following information security performance.

Output

(i) decisions related to continual improvement opportunities
(ii) decisions related to changes to the ISMS processes

Normative references

(i) Clause 9.3

4.6.4 Nonconformities and Corrective Action

In the occurrence of nonconformity, the organisation should react to the nonconformity and make corrections to control and deal with the consequences. Nonconformity refers to a "non-fulfilment of a requirement". Figure 4.28 illustrates the activity diagram in reacting to nonconformities and implementing corrective actions.

Input

(i) output from Assessment of Impacts View
(ii) output from Objectives Specification View
(iii) output from Monitoring and Measurement View
(iv) output from Internal Audit View

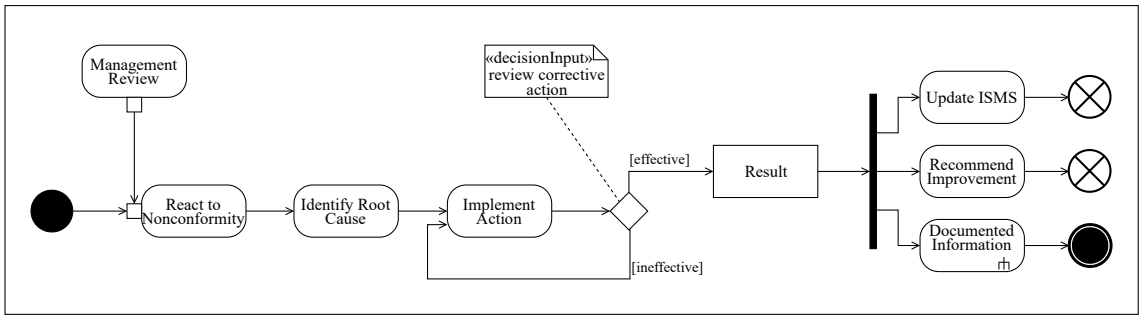


Figure 4.28: Activity diagram of Nonconformity and Corrective Action View

Activity

Nonconformities could occur in an organisation by a complete or partial non-fulfilment of a requirement of the standard, the lack of implementation of a necessary process or control relevant to the ISMS and non-compliance with legal or agreed customer requirements.

The organisation should develop a method for handling the nonconformities, and such an approach includes the identification of the non-fulfilment, identify the corrections to limit the impact of the nonconformity, implement the corrections as identified and review the effectiveness of the corrections.

Additionally, the organisation should define a handling process for corrective actions to manage the nonconformities by implementing the corrections. The organisation should identify the cause of the nonconformity to prevent recurrence of the nonconformity. The cause analysis enables the organisation to identify the root of nonconformity and provide opportunities to understand patterns and criteria that may cause a similar issue in the future. Corrective actions should be assessed to confirm if they are suitable for the cause of the nonconformity and prevent related nonconformities from occurring.

Output

(i) nature of nonconformity and taken correction
(ii) root cause of the nonconformity
(iii) result of corrective action

Normative references

(i) Clause 10.1

4.6.5 Continual Improvement

As mentioned earlier, the information security management system is a live process, and this includes continual improvement to the effectiveness of the process. Continual improvement refers to the ongoing effort to improve the performance of the ISMS. An activity diagram shown in Figure 4.29 demonstrates the processes

involved in the Continual Improvement View.

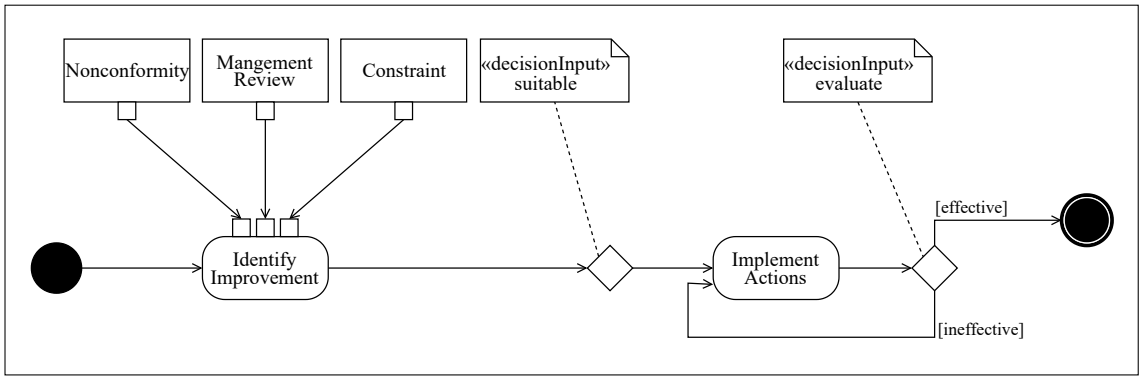


Figure 4.29: Activity diagram of Continual Improvement View

Input

(i) output from Constraints Specification View

(ii) output from Management Review View

(iii) output from Nonconformities and Corrective Action View

Activity

The processes discussed so far concerns with the implementation and current structure of the ISMS, however, continual improvement refers to the future shape of information security in organisations. It provides detailed or abstract direction on what should be achieved to improve the information security processes and enhance the reliability of the ISMS.

The organisation should continually look for opportunities to enhance the suitability, adequacy and effectiveness of the ISMS. The activity to continually improve the ISMS is often triggered following the result of the risk assessment or a raise of nonconformity. Other reasons that may provide opportunities for enhancement of the ISMS is changes to the constraints introduced by actors.

The identification areas of improvement should be assessed to evaluate if they are worth pursuing and its suitability for the ISMS. Once the proposed opportunity implements, changes to the ISMS should be determined. The organisation should evaluate the effectiveness of the actions and ensuring the benefits are realised as and nonconformities do not occur.

Output

(i) description for improvement

(ii) proposed action for continual improvement

Normative references

(i) Clause 10.2

4.7 Summary

This chapter introduced the INFORMS framework by providing principles and practices for using and implementing information security management systems. This included exploring the structure of the framework and a detailed description of viewpoints and views. It highlighted the workflow of the framework and association between each view. Next, it described methods in presenting the views followed by a generic structure of the views. It introduced the process in implementing and modelling each view, including the UML activity diagram, input, activity, output and the relative normative references for each view.

Chapter 5

Evaluation

In this chapter, the theoretical and practical components of INFORMS evaluated to prove that our proposed approach is a valid contribution in identifying, modelling and conforming to the requirements of the standard. The case study aims to demonstrate the expressiveness of the modelling language and the effectiveness of the framework, with an objective to plan and execute an unbiased and reliable evaluation exercise.

5.1 Evaluation Method

The perseverance consideration of the central role of people in using the framework was an integral part of the INFORMS development. Software engineering involves observation to technical as well as non-technical issues that often have to be taken into account in the design of empirical studies [131].

This thesis uses the hybrid methods based on DESMET methodology [132] to evaluate the proposed framework effectively, it separates the evaluation exercise into two types of:

Quantitative evaluation aimed at measuring the effectiveness of the proposed framework. It is an objective evaluation based on identifying the benefits of the framework in measurable term by determining whether INFORMS can support the implementation of the information security management systems.

Qualitative evaluation aimed at establishing the appropriateness of the framework. It is a subjective assessment of the specific features and characteristics provided by the framework, e.g., usability and effectiveness of INFORMS.

The evaluation procedure organised two techniques of a case study and a survey. In the case study, the framework was deployed on a real organisation to evaluate the effectiveness of the framework. It is planned to confirm or refute the aim of the proposed framework [133]. Benbasat [134] defines case study as an empirical enquiry that examines "a phenomenon in its natural setting, employing multiple methods

of data collection to gather information from one or a few entities (people, groups, or organization). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental control or manipulation is used."

In the survey, the same organisation that used the framework asked to provide information about the framework. Fink [135] defines survey as a comprehensive research method for gathering information to "describe, compare or explain knowledge, attitudes and behaviour". In this thesis, the users of the framework were asked through a semi-structured interview to provide information with respect to the properties of interest. The information was collected and analysed qualitatively, and it was done before and after the use of INFORMS in a retrospective manner using a direct technique, such as interviewing.

5.1.1 Case Study

A large-scale evaluation of the overall framework performed via the case study; this empirical evaluation provided us with unique insights about the overall applicability and effectiveness of the framework. The INFORMS framework applied to a private organisation, in close cooperation with system stakeholders, for the development of an information security management systems. Both quantitative and qualitative data from the application of the framework collected through the case study in the means of previously defined metrics and stakeholders interviews. In conducting the case study, five steps [136] were considered as a guideline for evaluating the framework, the steps included are as follow.

Case study design defined the objectives, and the case study was planned by identifying a range of elements in the design of the case study, e.g., rationale, units of analysis. The overall objective of the case study is to identify whether the developed framework can support the implementation of an information security management system in a real-life information system. A detailed explanation of the system and the stakeholders involved in this case study are discussed in Section 5.2.

Preparation for data collection defined procedures for data collection before the application of the framework. It performed in cooperation with some of the system's stakeholders following a semi-structured interview, where questions planned in a listed order depending on the development of conversation with the interviewee. The interviewees were encouraged to provide descriptive information about the organisation using the qualitative format. In addition to that, semi-quantitative analysis in Table 5.1 was delivered prior to the application of the framework to provide a metric on the readiness of the organisation.

Collecting evidence involved the execution of the data collection procedures as defined in the previous step. It required a large amount of raw data to be collected, refined and modelled using the INFORMS modelling language by the organisation's stakeholders. The data collected from the studied organisation during the execution of the framework for the creation of different models of the viewpoints and views illustrated in Section 5.3.

Analysis of collected data where the application of the framework analysed for the extraction of conclusions, this step held a qualitative evaluation of the framework's application through a semi-structured interview with the involved stakeholders in the implementation of the ISMS, as well as the evaluation of a semi-quantitative metrics in the post-implementation of the framework.

Reporting prepared to disseminate artefacts collected during the case study to summarise and draw conclusions on the findings of the evaluation. Results consisted of a brief discussion of the areas raised by the stakeholders during the exit interview and evaluation of the metrics presented in Section 5.4.

5.2 Case Study Design and Planning

The case study selected for the application of the developed framework involved a private organisation called Affordable Health Care (AHC) Limited[1] which provides health insurance products to individuals. AHC Limited established in 2005 in the UK and currently has ten employees located in one location; its annual turnover is between £1.5 to 2 million, and its customer base is in the UK.

AHC processes a lot of sensitive data from its clients to sell them or provide them with the services that they require, some of these data include:

- Personally Identifiable Information (PII), e.g., date of birth and home address.
- Special Data (SD), e.g., medical information and health records.
- Bank account and credit card details for payments.

Also, AHC processes sensitive data from its employees to comply with relevant laws and regulations, some of these data include:

- PII, e.g., date of birth and home address.
- Copy of passport and proof of residency.
- Records of qualification and training.
- Bank account details.

[1] real title was excluded and made anonymous for confidentiality

5.2.1 Objectives

The overall aim of the case study is to assess the developed framework to support the analysis and implementation of information security management system in a commercial setting. In specific, the objectives are as follow to:

- undertake the framework evaluation in a commercial setting using a case study evaluation method; and
- deploy the framework to manage the requirements of the ISO/IEC 27001.

The case study took place in a commercial setting; however, the secondary audience is academia.

5.2.2 Units of Analysis

The study of any framework similar to the extent of INFORMS is a challenging and timely task, which may produce uncertain evaluation results. As an approach to organising the evaluation of INFORMS, the case was logically divided into units to ensure the completeness of the details and avoid loss of crucial information.

An embedded case study as illustrated in Figure 5.1 adopted by [137] developed to anticipates the need to collect, analyse, and report on every viewpoint in the framework. Overall, the study could be characteristics as a single embedded case study with an overall case of the AHC.

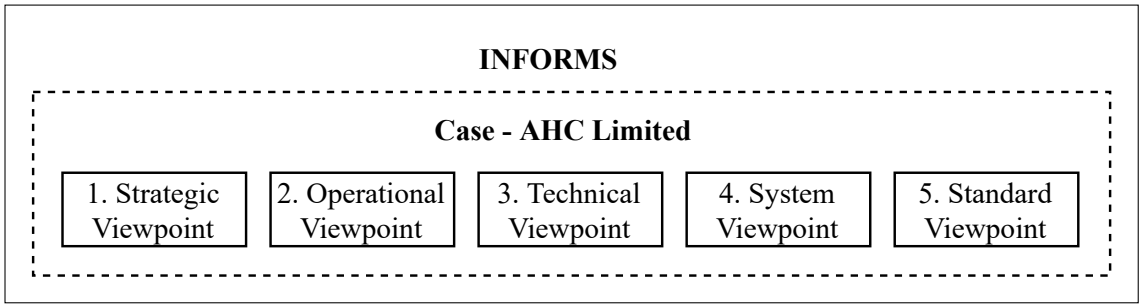


Figure 5.1: Overview of the context and units of analysis

5.2.3 Methods of Data Collection

The case study conducted within a collaboration program between the researcher and the organisation under study. Issues of confidentiality and publication were addressed in Ethical Considerations in Section 5.2.6. The researcher got access to the organisation's facilities and information systems at the same level as employees of the organisation, except access to the sensitive data of clients and employees.

The evaluation planned that the study should conduct in a series of iterative fashion with continuous feedback to complete all the areas of the study, as discussed

in Units of Analysis in Section 5.2.2. The principle decision on the method of data collection defined during the planning step based on Lethbridge et al. [138] technique, the process for data collection was divided into three categories as follow.

1. Direct method, where informal interviews held to provide a general understanding of the organisation. The primary source of information in this case study is the interviews performed with the team members of the studied organisation. The interviews executed as semi-structured interviews, more in the form of a discussion. Interesting information about the organisation's activities was followed up immediately with each interview subject. Adaptations primarily made to gain further information about the organisation in areas the interviewees felt necessary to discuss for this study. The data collected as meeting notes and the findings compiled into a qualitative and semi-quantitative structure.
2. Indirect method, where the organisation deployed the application of INFORMS to produce a set of information, including graphical models for each view.
3. Direct and Independent methods, where the author independently delivered a post-implementation analysis of the organisation to review the outputs from the use of the framework. Also, the participants in the application of the framework interviewed to gather information on their experience during the implementation process.

The involvement of the author throughout the application of the framework may introduce bias to the process. In order to reduce such effect, the involvement was limited to providing an overview of each view prior to its use by the participants and addressed any of their inquiries after the completion of each view. Upon completion of each viewpoint, the participants discussed their experience and identified potential aspects of the deliverables in need of further refinement.

5.2.4 Selection of Data

The case study developed and performed in connection with three participants of the organisation. One participant acted as the primary contact in providing information and referred to as implementer by using the INFORMS framework to implement the ISMS. He had no prior knowledge about the requirements of the standard as well as no background in information security. The second participant selected from the top management to support the decision making aspects of the information security management system and helped the implementer in the use of the framework, e.g., identifying the strategic policies related to information security. The third participant who maintains the information technology infrastructure of the organisation

invited to provide expert knowledge to the implementer, e.g., to support information security risk management.

An alternative source of data was the procedures and other information generated from the activities of the business in the studied organisation. Much information is produced and stored in the organisation that may not be evident or have enough time to extract them from the interviewee during one interview. The nature of the framework covers the operational aspect of the organisation; hence, it is useful to collect sufficient data from across the organisation.

5.2.5 Case Selection Strategy

One strategy in identifying the study context was selecting an organisation from the industrial collaboration network that the researcher can gain access to, based on mutual trust. The organisations were identified from the contact network of the researcher, and at the same time attempts were made to achieve maximum variation sampling to have a context where results can be generalised, e.g., size, domain and types of services.

The case itself decided based on availability; AHC Limited presented an opportunity to conduct an evaluation of INFORMS and to study that evaluation process. The identification and selection of activities in the organisation determined during the evaluation process.

5.2.6 Ethical Considerations

Due to the nature of the thesis, there was no requirement at the time at the respective University for ethics approval. An appropriate non-disclosure agreement was signed with the studied organisation and the individual researcher to ensure that confidential information was not disseminated outside the organisation. This agreement is binding beyond the duration of the research. It is crucial to ensure the secrecy of the interview records, organisation's information, and our trust and honour as a researcher are at stake if our promise on confidentiality is not kept. We believe that the trust that interviewees showed us largely depends on the ethical reputation of the involved university and the individual researcher's credibility.

5.2.7 Data Collection

The data collected through the use of the framework analysed both qualitatively and semi-quantitatively. The interviews were not recorded or transcribed, however, the researcher took notes of relevant information during the interviews. A methodical approach was employed to elicit information prior, during and after the application of INFORMS, it involved a number of actions including:

1. an initial discussion held with the stakeholders to introduce them with a high-level overview of the framework, explained the goal of the case study and initiated communications;
2. the stakeholders described the studied organisation, their business activities and their interdependencies;
3. a detailed explanation of the INFORMS modelling language, framework workflow, description of viewpoints and views, the use of Plugin for the modelling software platform was given to the implementer. It enabled the implementer to accumulate sufficient knowledge on the use of the proposed materials and had a preliminary understanding of the ISO/IEC 27001;
4. the researcher accompanied with the implementer to deliver a gap analysis to develop an accurate snapshot of the processes in the organisation;
5. a member of top management and the implementer provided input for the views in the Strategic Viewpoint;
6. the implementer provided information on the business processes and modelled the views in the Operational Viewpoint;
7. information security risk management delivered using INFORMS by the implementer and a representative of the IT contractor team to assist with security expertise;
8. the implementer modelled the requirement of the System Viewpoint;
9. views in Standard Viewpoint completed by a member of the top management and a representative of the IT contractor team, while the implementer supervised and modelled the process;
10. the researcher and the implementer carried the overall refinement of all actions between the steps 5 to 9;
11. all modelled processes and viewpoints collected from the organisation using a secure format, and transformation completed to ensure their alignment with the INFORMS modelling language;
12. an exit interview conducted to gather qualitative information about the experience of the participants; and
13. a post-implementation analysis carried out to produce a semi-quantitative report of the organisation using INFORMS for implementing an information security management system.

An exit interview with the participants of the case study provided qualitative insights regarding the perceived applicability and effectiveness of the proposed framework. The type of questions discussed during the interview was open-ended, including:

– How does the framework help the organisation achieve its objectives?
– How did you and the team use the framework?
– What is your favourite feature or part of the framework? Why?
– What challenges did you and your team experience during implementation?
– Any observations with regards to your specific perspective in the project?
– Do you have any feature requests or suggestions for improving the framework?

Additionally, a post-implementation analysis deployed to offer semi-quantitative insights regarding the framework's performance in the case study. More specifically, this analysis assessed the conformity of the organisation towards the requirements of the standard.

It included information used to implement the information security management system; therefore, the semi-quantitative metrics evaluated the completeness of the model transformation process and the qualitative feedback used to extract further insights regarding other aspects of the framework, e.g., usability and understandability.

Prior to the deployment of the framework on the studied system, a gap analysis as shown in Table 5.1 delivered to establish a baseline to compare the results' of the metrics against; it determined the overall readiness of the organisation. Additionally, it provided a snapshot of the organisation's actual performance with comparison to the requirements of the standard.

Part one of the table lists the mandatory documents and records that must be available in the organisation as per requirements of the standard; the second part lists the non-mandatory documents and records that are required as applicable to the ISMS and operation of the organisation. The documents and records refer to documented information and objective evidence to conform to clauses 4 to 10 of the standard as well as the applicable controls provided in Annex A of the standard.

The result of the investigation for each assessed area is shown in the status part of the table, which indicates the level of the organisation's readiness towards a particular document or record. As can be seen in the table, the AHC failed to fulfil most mandatory documents and records as required by the standard. Also, the organisation could not provide relevant evidence of the non-mandatory documents and records. Most security controls by the Annex A of the standard were missing in the organisation and putting the organisations and their information assets at risk.

Table 5.1: Gap analysis of the AHC's documents and records

Clause	Document/record	Status
Part 1: Mandatory		
4.3	Scope of the ISMS	-
5.2	Information security policy	-
4.3	Scope of the ISMS	-
5.2	Information security policy	-
6.1.2	Risk assessment and risk treatment methodology	-
6.1.3 d	Statement of Applicability	-
6.1.3 e	Risk treatment plan	-
6.2	Information security objectives	-
7.2	Records of training, skills, experience and qualifications	+
8.2	Risk assessment report	-
9.1	Monitoring and measurement results	-
9.2	Internal audit program	+
9.2	Results of internal audits	+
9.3	Results of the management review	+
10.1	Results of corrective actions	+
A.7.1.2 A.13.2.4	Definition of security roles and responsibilities	-
A.8.1.1	Inventory of assets	-
A.8.1.3	Acceptable use of assets	-
A.9.1.1	Access control policy	+
A.12.1.1	Operating procedures for IT management	-
A.12.4.1 A.12.4.3	Logs of user activities, exceptions, and security events	-
A.14.2.5	Secure system engineering principles	-
A.15.1.1	Supplier security policy	-
A.16.1.5	Incident management procedure	-
A.17.1.2	Business continuity procedures	-
A.18.1.1	Statutory, regulatory, and contractual requirements	-
Part 2: Non-mandatory		
7.5	Procedure for document control	-
7.5	Controls for managing records	-
9.2	Procedure for internal audit	+
10.1	Procedure for corrective action	+
A.6.2.1	Bring your own device (BYOD) policy	N/A

Continued on next page

Table 5.1: continued from previous page

Clause	Document/record	Status
A.6.2.1	Mobile device and teleworking policy	-
A.8.2.1 A.8.2.2 A.8.2.3	Information classification policy	+
A.8.3.2 A.11.2.7	Disposal and destruction policy	-
A.9.2.1 A.9.2.2 A.9.2.4 A.9.3.1 A.9.4.3	Password policy	-
A.11.1.5	Procedures for working in secure areas	-
A.11.2.9	Clear desk and clear screen policy	-
A.12.1.2 A.14.2.4	Change management policy	-
A.12.3.1	Backup policy	+
A.13.2.1 A.13.2.2 A.13.2.3	Information transfer policy	-
A.17.1.1	Business impact analysis	-
A.17.1.3	Exercising and testing plan	-

Note:
N/A = Not Applicable - = Not fulfilled
+ = Partially fulfilled ++ = Fulfilled

5.3 Application of Framework

The evaluation of the framework used the same work-flow as described in Section 4.1.1. The contents of Chapters 3 and 4 were available to the AHC, which they could access to a detailed description of the INFORMS modelling language and framework. The overall application of the framework was supervised by the researcher and supported with any enquiries or area of concern.

The AHC used the online version of the Draw.io platform, and the researcher gave a custom library of the INFORMS concepts to the organisation. The size of the graphical notations is not indicative of their importance; the sizes were adjusted to reduce line crossings and bends to make the diagrams more natural to understand.

5.3.1 Strategic Viewpoint

A representative of the top management implemented this viewpoint in the AHC, the implementation of the views in the Strategic Viewpoint requires input and influence of the organisation's leadership. It is reasonable for the top management's representative to be involved in the decision-making activities in the Strategic Viewpoint.

Scope

The purpose of the Scope View is to define the boundaries of the ISMS in AHC in order to decide what services require protection. The scope of the ISMS established after taking into account the legal, regulatory, contractual, and other requirements, and specified by including the following items:

- All physical and information assets owned by the AHC Limited.
- Services, support and data provided to clients.
- Data provided by the clients, employees and partners.
- All staff, including the director.

Leadership

The top management agreed to:

1. meet their obligatory duties in the ISMS;
2. participate in the development of the information security policy and ensure the policy is in line with the strategic direction of the AHC;
3. assist in establishing information security objectives;
4. invest up to £10,000 for the implementation of the ISMS;
5. provide required resources as necessary for the ISMS;
6. assign the roles and responsibilities to relevant persons and direct them to achieve the intended outcomes of the ISMS;
7. take an active part in promoting continual improvement of the ISMS;
8. communicate the importance of effective information security management; and
9. attend a management review meeting at least every semester with preferring every quarterly if all the members of the required team are available.

Policy

The following is the information security policy produced by the AHC's top management:

> "Affordable Health Care (AHC) Limited located in London, United Kingdom, which operates in the insurance sector are committed to preserving the confidentiality, integrity and availability of all the physical

and electronic information assets throughout the business in order to preserve our competitive edge, profitability, legal, regulatory and contractual compliance and commercial image. Information security requirements will continue to align with our business objectives and the ISMS is intended to be an enabling mechanism for the operation of the AHC.

Our current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of the ISMS. All employees of AHC Limited are expected to comply with this policy and receive appropriate training. A current version of this document is available to all members of staff on AHC Intranet and office. It does not contain confidential information and can release to relevant external parties.

This information security policy was approved by the AHC Limited director."

Awareness

The top management developed an extensive awareness and training programme following the establishment of the information security policy, which the AHC committed to promoting appropriate training to its employees. The organisation had to ensure that such a programme will have a contribution to the effectiveness of the ISMS and performance of information security.

The organisation identified a series of activities to implement throughout the year and provided a planned programme shown in Table 5.2. AHC identified five methods for information security awareness, education, and training programme, including Information day, Email newsletters, Intranet articles, E-learning, and Video blogs. The methods planned throughout the year to enhance their effectiveness; the organisation wanted to have a minimum of one activity per month to regularly inspires the importance of information security.

The top management decided to assign the Office Manager as the custodian role with responsibility to successfully prepare and deliver the awareness and training materials as found in the awareness programme.

Communication

Due to the size of the organisation, the top management determined that one person is sufficient to be responsible for communications. The Office Manager was assigned with the custodian role to effectively communicate using appropriate chan-

Table 5.2: Annual awareness and education programme - AHC

Method	Information day	Email newsletter	Intranet article	E-learning	Video
January	+	+			
February		+	+		
March		+			+
April		+	+		
May		+		+	
June		+	+		
July		+			+
August	+	+	+		
September		+			
October		+	+		
November		+		+	
December		+	+		

nels with the internal and external interested parties. The methods of communication should always be delivered in writing either via emails or post.

Documented Information

The organisation developed a checklist used to create and maintain the documented information. The checklist as shown in Table 5.3 identifies all the required documented information in INFORMS as well as those generated by the organisation.

This approach ensures the organisation has all the necessary documents and records for meeting the requirement of the standard. The status column in the table address three stages in the preparation of a document including allocated, draft, and approved. This enables to trace and follow up the steps where a document exists. The top management decided to assign the Office Manager as the custodian role with responsibility to successfully create and maintain the documented information as expected by the standard.

Table 5.3: Documented information checklist - AHC

Description	Status		
	Allocated	Draft	Approved
Policy			+
Awareness			+
Communication			+
Documented Information			+
Actors Description			+
Constraints Specification			+
Asset Management			+
Assessment of Impacts			+
Risk Determination			+
Risk Evaluation			+
Risk Treatment			+
Risk Acceptance			+
Roles Description		+	
Objectives Specification			+
Monitoring & Measurement		+	
Internal Audit	+		
Management Review	+		
Nonconformity & Corrective Action	+		
Continual Improvement	+		

5.3.2 Operational Viewpoint

The implementer was the key contributor in identifying the information for the views in the Operational Viewpoint; this was modelled using a set of diagrams as illustrated in Figure 5.2. The overall model of the Operational Viewpoint drawn into smaller diagrams categorised per relevant actor, e.g., Director, Office Manager, Client. This enabled better management of the complex models, enhance readability and demonstrate a more precise output. The following sections describe each view and their modelling process of the AHC operation.

Actors Description

Main actors, including AC1, AC2 and AC3 are the key actors in the business function of the organisation. While all three actors are an employee of the AHC, the top management decided to classify personnel based on their job profile; the Office Manager (AC2) was assigned a separate actor's ID to the Support Personnel (AC3). The organisation has a partnership with a Health Insurance Partner (AC5) to provide its products and services to AHC's Clients (AC4).

Due to the size of the organisation, top management decided to outsource its IT infrastructure to an IT Contractor (AC13), who maintains the overall IT needs of the organisation. Similarly, the organisation's website and its on-line operation maintain by a Hosting Provider (AC10). The organisation identified all the legal and regulatory actors applicable to the nature of the business. Apart from generic actors such as AC14, AC15 and AC16, there are other actors including AC17, AC18, and AC19 that audit the activities of the organisation; AHC is legally required to comply with their requirements.

The organisation identified the types of actors, all personnel, including the director classed as internal while the remaining actors are external. AHC determined that all internal actors have the required competency in doing their tasks. The level of granularity of modelling actors in INFORMS is an organisational decision; the organisation could define as many or few as possible. However, it needs to include all relevant actors to the ISMS. A list of all actors discussed above is presented in Table 5.4.

Table 5.4: Description of the actors - AHC

ID	**Description**	**Type**	**Competency**
AC1	Director	Internal	True
AC2	Office manager	Internal	True
AC3	Support personnel	Internal	True
AC4	Client	External	N/A
AC5	Health Insurance Partner (HIP)	External	N/A
AC6	Electricity provider	External	N/A
AC7	Telephone provider	External	N/A
AC8	Water provider	External	N/A
AC9	Building insurance	External	N/A
AC10	Hosting provider	External	N/A
AC11	Accountant	External	True
AC12	Business advisor	External	True
AC13	IT contractor	External	True
AC14	EU GDPR	External	N/A
AC15	HMRC	External	N/A
AC16	Companies House	External	N/A
AC17	Information Commissioners Office (ICO)	External	N/A
AC18	Financial Conduct Authority (FCA)	External	N/A
AC19	Financial Ombudsmen Services (FOS)	External	N/A

Constraints Specification

The implementer identified the actors by considering the interested parties to the organisation and the ISMS. Most actors were apparent to the organisation, while others such as AC14, AC18, and AC19 required a thorough assessment for their applicability to the ISMS.

The organisation identified 21 constraints applicable to the ISMS. Some actors express more than one constraint, and some had none, it depends on the organisation to identify those constraints by considering the issues and the context of the organisation. For example, the Director (AC1) introduced three constraints including C1, C3, and C4, which two are advisory and C4 is obligatory. C4 describes that "All processes that put the organisation in liability must be approved by the top management", this constraint restricts the goals which put the organisation at liability, and they must have the necessary approval from the top management before proceeding.

AHC identified nine out of 21 constraints as advisory. It is noted that those constraints instructed by the legal and regulatory actors are mainly obligatory except some that provide some degree of flexibility to the organisation. For example, C20 introduced by the Financial Conduct Authority (AC18) suggests the organisation to provide "training and awareness" to its personnel; however, it does not explicitly require the organisation to provide training and awareness. Similarly, C21 is another constraint by AC18 that suggests the organisation to pay attention to "data backup".

Other sets of constraints which were obliged to the organisation are the requirements of the GDPR (AC14), which indicates eight obligatory constraints to be satisfied by the organisation regarding the private data of its clients and personnel of the AHC. A list of all constraints introduced by the actors is provided in Table 5.5.

Asset Management

AHC identified 26 asset categories for the organisation. As part of the asset management, the organisation identified the risk owners and custodians for each asset category. While all assets require risk ownership, it is not mandatory to assign a custodian role for each asset. For example, the risk owner for the Server room (A2) is Director (AC1), and the custodian is Building insurance (AC9). Table 5.6 shows an inventory of assets including classification, risk owner and custodian.

Table 5.5: Specification of the constraints - AHC

ID	Description	Actor	Type
C1	All correspondences must be secured when includes PII and SD	AC1	Advisory
C2	Personal data to insurance product providers, both in paper form and online must be via a secure portal	AC5	Advisory
C3	All restricted asset category must have an Access Rights Policy	AC1	Advisory
C4	All processes that put the organisation in liability must be approved by the top management	AC1	Obligatory
C5	Personal data to be accessed by employees and partners within the firm only	AC4	Advisory
C6	Personal data will only be used for the purposes to provide requested services	AC4	Advisory
C7	Lawful basis for collecting and using personal data	AC14	Obligatory
C8	Transparent use of personal data	AC14	Obligatory
C9	Individuals are clear about the purpose of processing their information	AC14	Obligatory
C10	Data gathering is adequate, relevant, and limited to what is necessary	AC14	Obligatory
C11	Information is kept accurate and updated	AC14	Obligatory
C12	Employment records to be deleted after six years	AC3	Advisory
C13	All records must be kept for at least five years	AC15	Obligatory
C14	Information must not be kept for longer than is needed	AC14	Obligatory
C15	Do not disclose any confidential information without the prior written consent of the other party	AC5	Advisory
C16	Register a DPO	AC17	Obligatory
C17	Integrity and confidentiality of data is maintained	AC14	Obligatory
C18	Responsibility of what you do with personal data	AC14	Obligatory
C19	Report a breach of information	AC17	Obligatory
C20	Training and awareness	AC18	Advisory
C21	Data back-up	AC18	Advisory

Table 5.6: Inventory of assets - AHC

ID	Description	Classification	Risk owner	Custodian
A1	Building Reception Sales office	Sensitive	AC1	AC9
A2	Server room	Confidential	AC1	AC9
A3	Branding Reputation	Public	AC1	-
A4	Client list	Confidential	AC1	-
A5	Software license	Confidential	AC2	AC13
A6	Supplier/Partner agreement Legal correspondences	Confidential	AC1	AC12
A7	Invoice Bank statement PAYE	Confidential	AC2	AC11
A8	Pricing term Quote report	Sensitive	AC2	-
A9	Treatment instruction	Confidential	AC2	-
A10	Client Special Data	Confidential	AC1	AC2
A11	Employment record	Confidential	AC1	AC2
A12	Client agreement	Confidential	AC1	AC2
A13	Medical claim	Sensitive	AC1	AC2
A14	Personnel PII Client PII	Sensitive	AC1	AC2
A15	Telephone Broadband	Sensitive	AC1	AC7
A16	Electricity supplies	Sensitive	AC1	AC6
A17	Water supplies	Sensitive	AC1	AC8
A18	Web hosting Domain Contact form	Public	AC1	AC10
A19	Director Operation manager Support personnel	Public	AC1	-
A20	Microsoft Windows 7 Server 2003	Confidential	AC2	AC13

Continued on next page

Table 5.6: continued from previous page

ID	Description	Classification	Risk owner	Custodian
A21	CRM Microsoft Office Exchange server Antivirus	Sensitive	AC2	AC13
A22	Backups Hard drives Removable drives	Confidential	AC2	AC13
A23	FTP Files Email	Confidential	AC2	AC13
A24	Workstations HP Printer Wireless adaptor	Sensitive	AC2	AC13
A25	Apple iPad Acer laptop	Sensitive	AC2	AC13
A26	Telephone Fax	Sensitive	AC2	AC13

Goal Delivery

AHC identified 31 goals from their operational activities, and some of these goals refer to more than one asset or actor. For example, the goal "Provide a secure trading environment" (G1) introduced by Director (AC1) involves four assets A1, A15, A16, and A17. Therefore, the organisation only assigned one ID for this particular goal. On the other hand, the goal "Minimise litigation" (G2) introduced by Director (AC1) only requires one asset (A2) for its fulfilment. The implementer defined each goal based on the area of business operation and identified the required asset to deliver such goals.

The implementer identified the dependency of each goal concerning another goal or asset. Most goals did not require many dependencies since the implementer modelled a detailed analysis of the organisation's activities while there were some exceptions including G18, G20, G27, G28, etc.

The implementer assigned the identified constraints from Section 5.3.2 to each identified goal. Two lists of constraints shown in Table 5.7 to emphasise that some constraints restrict the assets and others restrict the goals. The Constraint (Asset) column refers to those constraints specifically restrict assets in fulfilling the cor-

responding goal, and the constraint (Goal) column refers to those constraints that restrict the goal itself. For example, Support Personnel (AC3) needs to fulfil a goal "record client SD" (G14) through CRM software (A21) to record client's (AC4) Special Data (A10); therefore, Support Personnel (AC3) depends on the client's Special Data to fulfil G14. Additionally, constraints (C6, C17, C18) restrict the use of Special Data (A10), and constraints C10 and C16 restrict the goal of recording client SD (G14).

Table 5.7 set out a full description of each goal including corresponding actor, asset, dependency and relevant constraints.

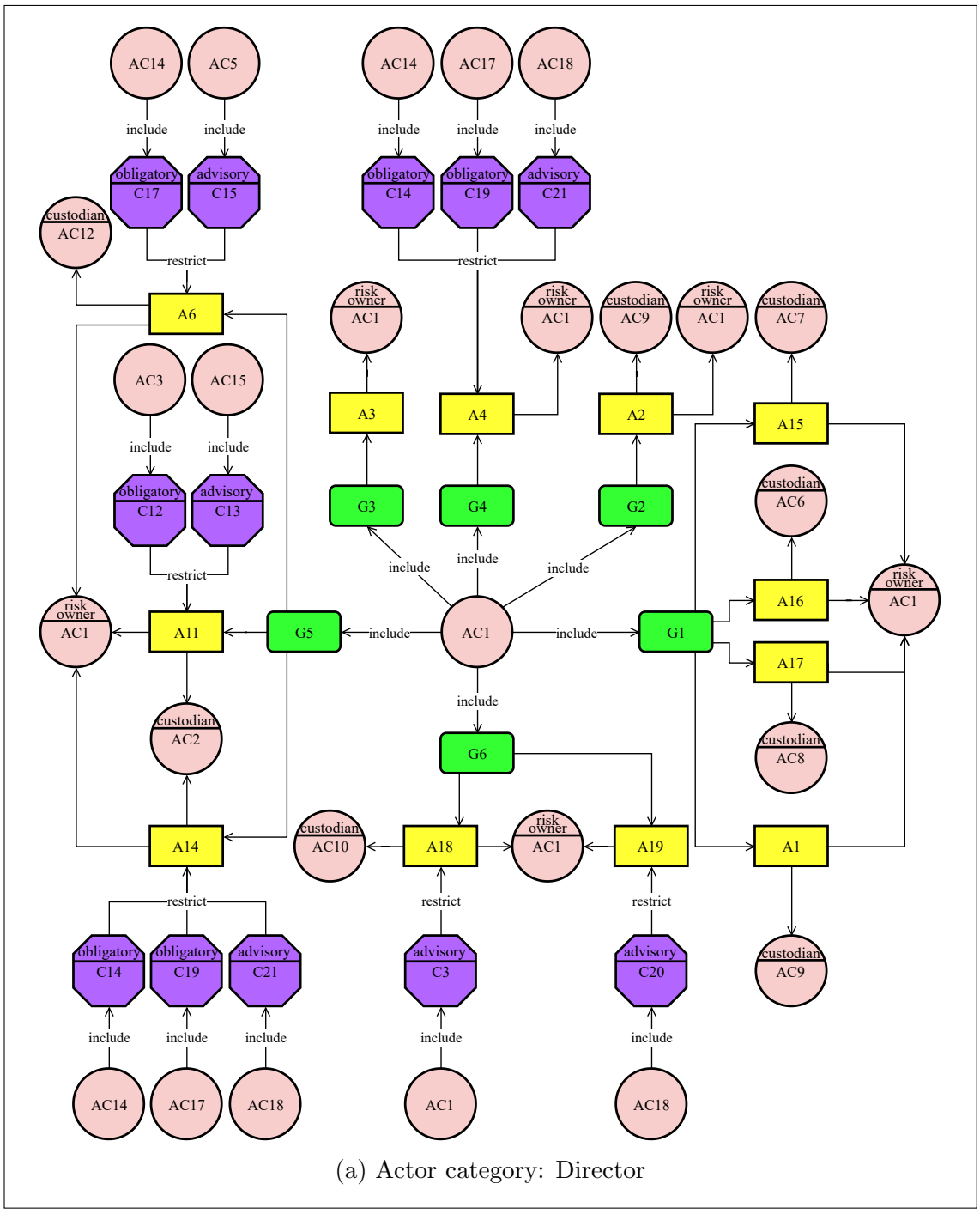
Table 5.7: Goals and dependencies - AHC

ID	Description	Actor	Asset	Dependee	Dependum	Constraint (Asset)	Constraint (Goal)
G1	Provide a secure trading environment	AC1	A1	-	-	-	-
G1	Provide a secure trading environment	AC1	A15	-	-	-	-
G1	Provide a secure trading environment	AC1	A16	-	-	-	-
G1	Provide a secure trading environment	AC1	A17	-	-	-	-
G2	Minimise litigation	AC1	A2	-	-	-	-
G3	Competitive advantage	AC1	A3	-	-	-	-
G4	Protect trade secret	AC1	A4	-	-	C14, C19, C21	-
G5	Support legal compliance	AC1	A6	-	-	C15, C17	-
G5	Support legal compliance	AC1	A11	-	-	C12, C13	-
G5	Support legal compliance	AC1	A14	-	-	C14, C18, C19	-
G5	Support legal compliance	AC2	A5	-	-	-	-
G5	Support legal compliance	AC2	A7	-	-	C13	-
G6	Meet commercial targets	AC1	A19	-	-	C20	-
G6	Meet commercial targets	AC1	A18	-	-	C3	-
G7	Improve productivity	AC2	A20	-	-	-	-
G7	Improve productivity	AC2	A21	-	-	-	-
G7	Improve productivity	AC2	A22	-	-	C18	-

Continued on next page

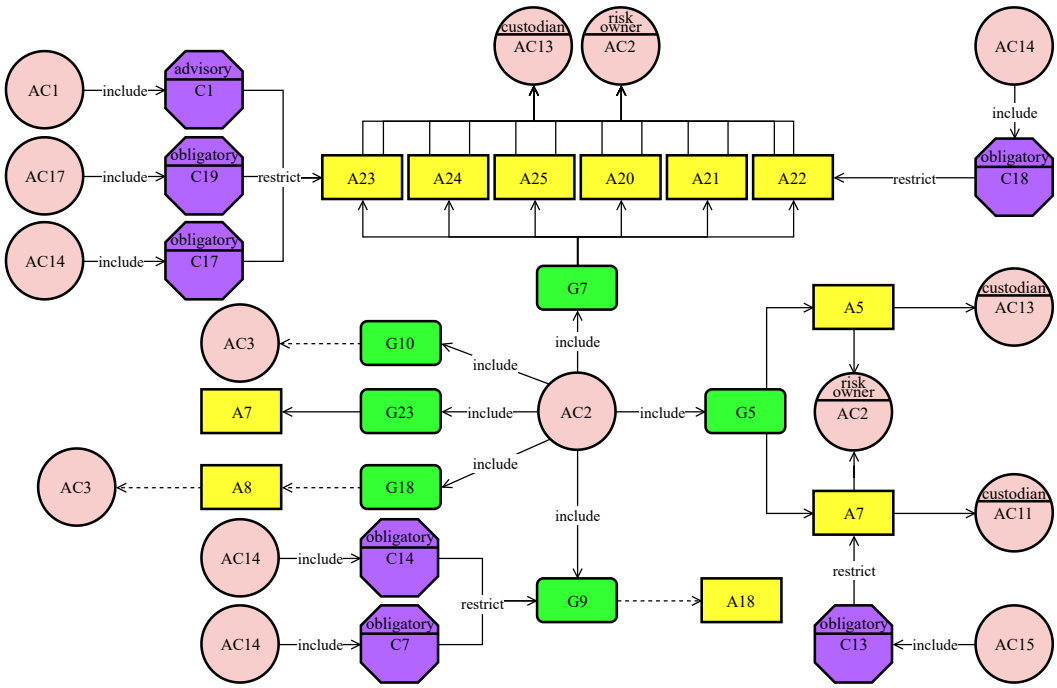
Table 5.7: continued from previous page

ID	Description	Actor	Asset	Dependee	Dependum	Constraint (Asset)	Constraint (Goal)
G7	Improve productivity	AC2	A23	-	-	C1, C19, C17	-
G7	Improve productivity	AC2	A25	-	-	-	-
G7	Improve productivity	AC2	A24	-	-	-	-
G8	Send enquiry	AC4	A14	A18	-	C14, C18, C19	C9, C6
G9	Receive Client enquiry	AC2	-	A18	-	-	C7, C14
G10	Assign sales lead	AC2	-	AC3	-	-	-
G11	Receive sales lead	AC3	-	AC2	-	-	-
G12	Contact potential lead	AC3	A26	-	-	-	C6, C9
G13	Provide SD	AC4	A10	AC3	-	-	C5,C9
G14	Record client SD	AC3	A21	AC4	A10	C6, C17, C18	C10, C16
G15	Share SD with HIP	AC3	-	AC4	A10	-	C2, C3, C9
G16	Provide pricing condition	AC5	A8	AC3	-	-	-
G17	Prepare quote report	AC3	A8	-	A21	-	-
G18	Approve quote report	AC2	-	AC3	A8	-	-
G19	Submit quote report	AC3	-	-	A8	-	C4, C7
G20	Receive client approval	AC3	-	AC4	A12	-	-
G21	Issue invoice	AC3	A7	-	-	C13	-
G22	Make payment	AC4	-	AC3	A7	-	-
G23	Approve receipt of payment	AC2	A7	-	-	-	-
G24	Issue HIP agreement	AC3	A6	-	-	-	-
G25	Approve HIP agreement	AC5	-	AC3	A6	-	-
G26	Make claim	AC4	A13	AC3	-	C6, C8	C6
G27	Notify claim to HIP	AC3	-	AC5	A13	-	C1, C2, C17
G28	Validate client claim	AC5	-	AC3	A13	-	-
G29	Issue treatment instruction	AC5	A9	AC3	-	C15	-
G30	Instruct medical treatment	AC3	-	AC5	A9	-	C1, C2, C20
G31	Receive medical treatment	AC4	-	AC3	A9	-	C14

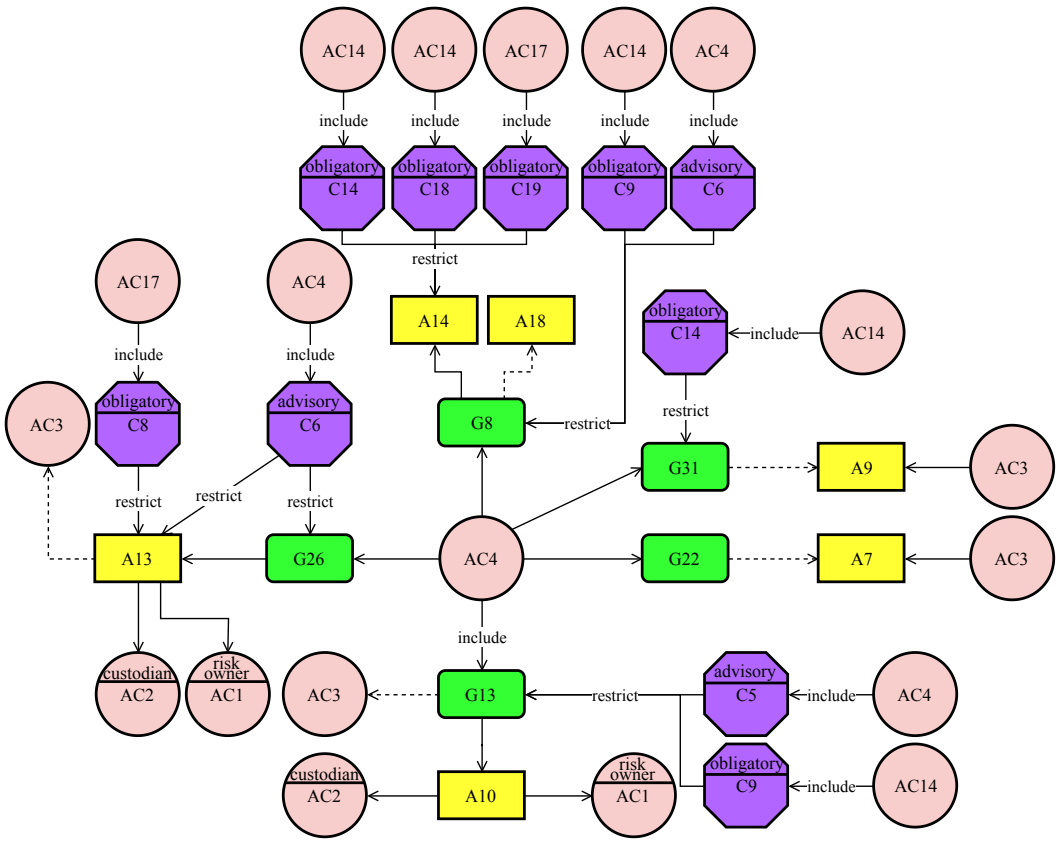


(a) Actor category: Director

Figure 5.2: Operational Viewpoint - AHC

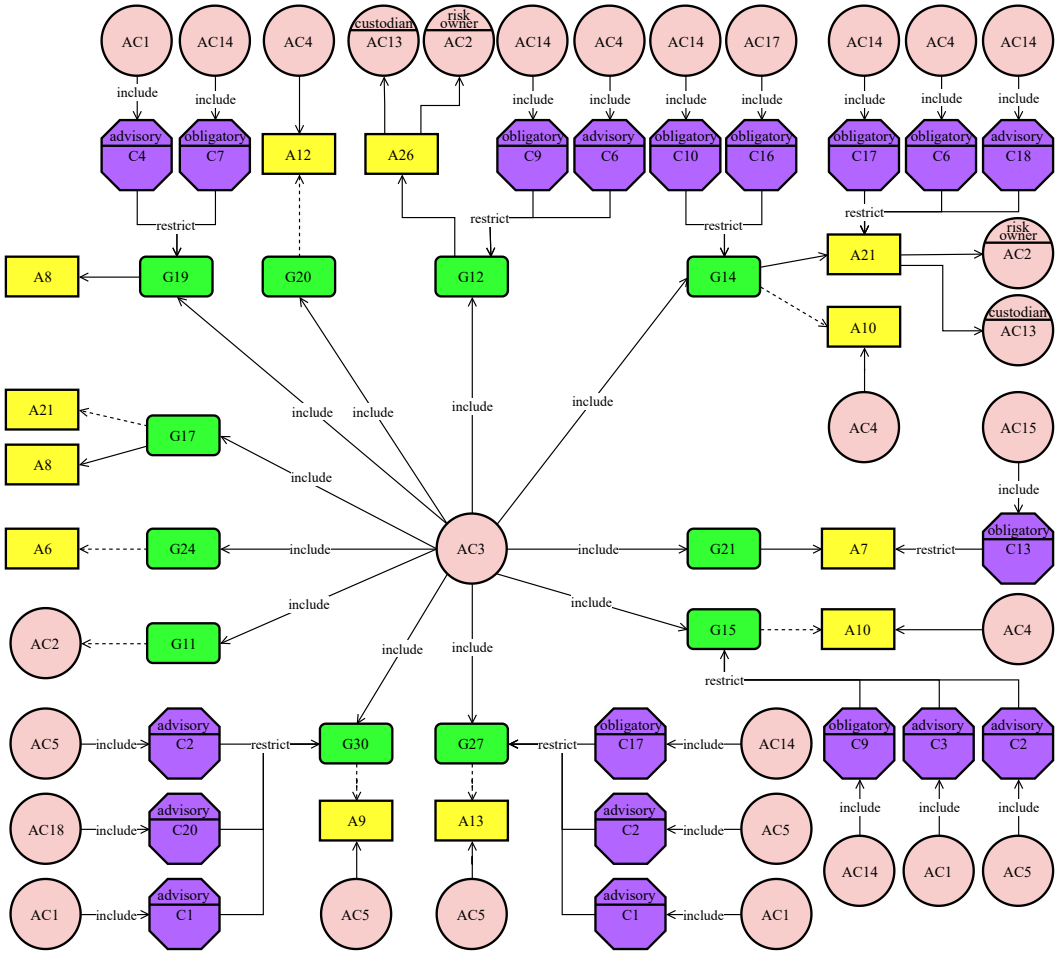


(b) Actor category: Office Manager

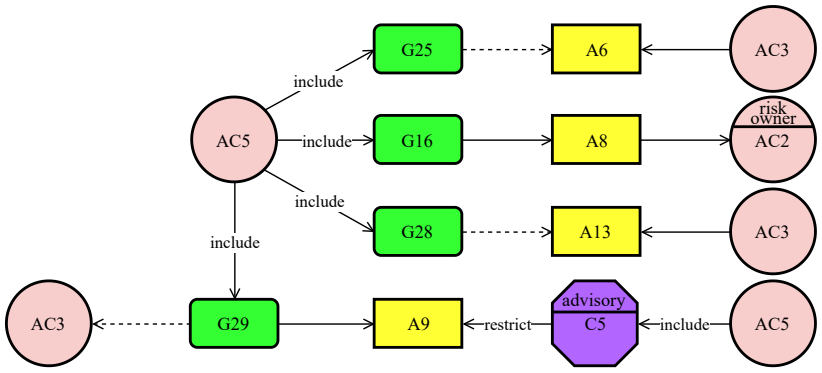


(c) Actor category: Client

Figure 5.2: Operational Viewpoint (cont.)



(d) Actor category: Support Personnel



(e) Actor category: Health Insurance Partner (HIP)

Figure 5.2: Operational Viewpoint

5.3.3 Technical Viewpoint

The modelling of the viewpoint is illustrated in Figure 5.3, where each risk assessed and treated using a set of diagrams. The overall model of the Technical Viewpoint drawn into smaller diagrams per risk scenario categorised into relevant goals, some of these goals grouped to illustrate a better representation and analysis of the risk scenarios, e.g., Sales Enquiry, Claim Management. The following seven sections describe each view and their modelling process of AHC risk management.

The participants involved in the implementation of the Technical Viewpoint were a representative of the top management, an expert member in information security and the implementer collectively assisted with the modelling of the Technical Viewpoint. The implementer noted that the Technical Viewpoint required deliberations by all involved participants. For example, the expert member initially proposed around 70 risk scenarios according to a number of threats and vulnerabilities that could harm the assets while the member of the top management concerned of their impact on the defined goals and actors of the organisation. Finally, a total of 45 risks conclusively confirmed by all participants.

Threats Identification

A representative of the top management who is also a risk owner to most assets assisted the expert member in identifying the threats to information security that could impact the assets and goals of the organisation. The degree of frequency for each threat established using the likelihood level defined in Table 4.3. AHC used the threat catalogue provided in Appendix A to support the selection of threats; however, the organisation was unrestricted to use any sources or methods to help the identification process.

Table 5.8 sets out the breakdown of all threats identified in a possible risk scenario impacting relevant goals and assets in the organisation. Each column shows a set of details which generated during the modelling process. It provides a threat ID, description of the threat, level of likelihood, a unique ID for a particular risk scenario and corresponding goal and asset. For example, malicious software assigned with a unique threat ID of (T65), a "medium" (3) level of likelihood, assigned with a unique risk ID of (R8) affecting "receive client approval" (G20) and "client agreement" (A12).

It is noted that the risk ID provided in the table is generated in incremental order, while the threat ID corresponds to a particular reference number in the aforementioned threat catalogue. AHC was able to assign any reference number as appropriate to the need of the organisation for both risk scenario and threat IDs.

Table 5.8: Threats and likelihoods - AHC

ID	Description	Likelihood	Risk	Goal	Asset
T100	Vandalism	1	R1	G1	A1
T94	Unauthorized installation of software	2	R2	G2	A2
T5	Breach of contractual relations	2	R3	G3	A3
T10	Compromising confidential information	2	R4	G4	A4
T70	Misuse of resources	1	R5	G4	A4
T74	Recovery of information from disposed media	1	R6	G5	A6
T45	Fraud	1	R7	G5	A6
T65	Malicious software (e.g., viruses)	3	R8	G20	A12
T5	Breach of contractual relations	1	R9	G24	A6
T76	Repudiation	3	R10	G24	A6
T56	Interruption of business processes	2	R11	G10	A14
T50	Illegal processing of data	3	R12	G11	A14
T10	Compromising confidential information	3	R13	G14	A10
T54	Information leakage	1	R14	G15	A10
T56	Interruption of business processes	3	R15	G26	A13
T41	Falsification of records	1	R16	G27	A13
T92	Unauthorized changes of records	1	R17	G5	A14
T69	Misuse of information systems	3	R18	G5	A14
T24	Disclosure of information	4	R19	G5	A11
T88	Traffic overloading	1	R20	G1	A15
T73	Power fluctuation	2	R21	G1	A16
T39	Failure of water supply	1	R22	G1	A17
T18	Defacement	2	R23	G6	A18
T40	Failure of website	1	R24	G9	A18
T45	Fraud	1	R25	G6	A19
T71	Operational support staff error	4	R26	G6	A19
T74	Recovery of information from disposed media	1	R27	G5	A5
T28	Eavesdropping	4	R28	G9	A18
T66	Masquerading of user identity	2	R29	G19	A23
T61	Loss of system integrity	1	R30	G12	A26

Vulnerabilities Identification

A representative of the top management and the expert member identified the vulnerabilities that could be harmful in a particular risk scenario. The exploitability of each vulnerability assessed using the ease of exploit level defined in Table 4.4. AHC used the vulnerability catalogue provided in Appendix B to support the

selection of vulnerabilities; however, the organisation was unrestricted to use any sources or methods to support the identification process.

Table 5.9 shows all identified vulnerabilities that could be exploited in a possible risk scenario impacting the organisation. Each column provides a set of details which generated during the modelling process. It describes a vulnerability ID, description of the vulnerability, level of ease of exploit, a risk ID matching to the corresponding risk identifier defined in the Identification of Threats View, as well as the corresponding goal and asset in a particular risk scenario. Following the example in the previous view, the risk ID (R8) assessed and identified that the "lack of anti-virus and malware prevention" (V44) could be a vulnerability to the assets and goals with "high" (4) ease of exploitability harm "receive client approval" (G20) and "client agreement" (A12).

Again, as noted previously in the Identification of Threats View, the risk ID provided in the table is generated in incremental order, while the vulnerability ID corresponds to a particular reference number in the aforementioned vulnerability catalogue. AHC was able to assign any reference number as appropriate to the need of the organisation for both risk scenario and vulnerability IDs.

Table 5.9: Vulnerabilities and ease of exploits - AHC

ID	Description	Ease of exploit	Risk	Goal	Asset
V60	Lack of physical protection of the building, doors and windows	4	R1	G1	A1
V13	Inadequate control of physical access	3	R2	G2	A2
V35	Insufficient contingency planning	1	R3	G3	A3
V87	Uncontrolled copying of data	3	R4	G4	A4
V91	Unmotivated employees	2	R5	G4	A4
V36	Insufficient enforcement of secure deletion and disposal process	2	R6	G5	A6
V16	Inadequate internal/external audit	2	R7	G5	A6
V44	Lack of anti-virus and Malware Prevention	4	R8	G20	A12
V45	Lack of audit trail	1	R9	G24	A6
V64	Lack of proof of sending or receiving messages	3	R10	G24	A6
V7	Failure to adhere to company policies	2	R11	G10	A14
V24	Inadequate security awareness	3	R12	G11	A14
V47	Lack of clean desk and clear screen policy	4	R13	G14	A10
V92	Unprotected communication link	3	R14	G15	A10
V71	Lack of validation of the processed data	3	R15	G26	A13

Continued on next page

Table 5.9: continued from previous page

ID	Description	Ease of exploit	Risk	Goal	Asset
V34	Insufficient change control process leading to unauthorized changes	3	R16	G27	A13
V34	Insufficient change control process leading to unauthorized changes	3	R17	G5	A14
V43	Lack of access control policy	3	R18	G5	A14
V87	Uncontrolled copying of data	3	R19	G5	A11
V66	Lack of redundancy	2	R20	G1	A15
V83	Susceptibility to voltage variations	2	R21	G1	A16
V40	Insufficient or irregular water supply	1	R22	G1	A17
V4	Default passwords not changed	3	R23	G6	A18
V17	Inadequate maintenance	2	R24	G9	A18
V84	Too much power in one person	1	R25	G6	A19
V28	Inadequate supervision of employees	3	R26	G6	A19
V5	Disposal of storage media without deleting data	3	R27	G5	A5
V92	Unprotected communication link	4	R28	G9	A18
V24	Inadequate security awareness	4	R29	G19	A23
V99	Untraceable user actions due to generic accounts	2	R30	G12	A26

Assessment of Impacts

The participants analysed the consequence of each risk to assets and goals. The measurement of impacts assessed using the level definitions in Table 4.5, based on the elements of assets, including confidentiality, integrity and availability. Similarly, the measurement of impacts assessed using the level definitions in Table 4.6, based on the elements of goals, including business, financial, legal, physical, privacy, social and technical. Following the assessment of impacts, the participants calculated the impact using the matrix shown in Table 4.7 to determine semi-quantitative values for Asset Impact Indicator (AII) and Goal Impact Indicator (GII).

Table 5.10 provided the assessment of impacts on assets and goals in AHC. Each column incorporates the relevant risk ID matching to the corresponding risk identifier defined in the Identification of Threats View, the corresponding threat, vulnerability, levels of likelihood and ease of exploit. Further, it contains a qualitative value indicating the consequence on each asset and goal element following the presentation of values for AII and GII.

Following the example discussed in the previous view, the risk (R8) has the following consequences on the asset's (A12) elements; the impact on the confidentiality is high (H), integrity is medium (M), and availability is high (H). Similarly, risk (R8) has the following consequences on the goal's (G20) elements; the impact on the business is medium (M), financial is low (L), legal is medium (M), physical is low (L), privacy is medium (M), social is low (L) and technical is medium (M).

Next, AHC used the threat's (T65) likelihood, the vulnerability's (V44) ease of exploit and the above level of impacts to calculate the AII and GII using the aforesaid matrix table. This established the semi-quantitative values for each element of the assets and goals. The calculation of the impact to each element of the asset determined value for the confidentiality is (8), integrity is (7) and availability is (8). The calculation of the GII determined the indicator value for the business is (7), financial is (6), legal is (7), physical is (6), privacy is (7), social is (6) and technical is (7). The determination of all values results in AII{8,7,8} and GII{7,6,7,6,7,6,7}.

Table 5.10: Assessment of impacts - AHC

					Impact (Asset)			**Impact (Goal)**							**AII**			**GII**						
ID	Threat	Vulnerability	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical
R1	T100	V60	1	4	L	M	H	M	L	L	M	L	L	M	4	5	6	5	4	4	5	4	4	5
R2	T94	V13	2	3	H	M	M	L	L	L	L	M	L	H	6	5	5	4	4	4	4	5	4	6
R3	T5	V35	2	1	L	H	H	M	M	M	M	L	L	M	2	4	4	3	3	3	3	2	2	3
R4	T10	V87	2	3	H	H	M	M	M	H	L	H	L	M	6	6	5	5	5	6	4	6	4	5
R5	T70	V91	1	2	H	H	M	L	H	M	L	H	L	M	4	4	3	2	4	3	2	4	2	3
R6	T74	V36	1	2	H	H	M	L	L	M	L	M	L	M	4	4	3	2	2	3	2	3	2	3
R7	T45	V16	1	2	M	H	M	M	L	L	L	L	L	L	3	4	3	3	2	2	2	2	2	2
R8	T65	V44	3	4	H	M	H	M	L	M	L	M	L	M	8	7	8	7	6	7	6	7	6	7
R9	T5	V45	1	1	M	M	M	L	L	M	L	L	L	M	2	2	2	1	1	2	1	1	1	2
R10	T76	V64	3	3	M	M	M	M	H	M	L	L	L	M	6	6	6	6	7	6	5	5	5	6
R11	T56	V7	2	2	M	H	H	M	L	M	L	M	L	M	4	5	5	4	3	4	3	4	3	4
R12	T50	V24	3	3	M	H	H	M	M	H	L	H	L	M	6	7	7	6	6	7	5	7	5	6
R13	T10	V47	3	4	H	H	M	L	H	M	L	M	L	M	8	8	7	6	8	7	6	7	6	7
R14	T54	V92	1	3	H	H	M	L	M	M	L	H	L	M	5	5	4	3	4	4	3	5	3	4
R15	T56	V71	3	3	H	M	H	L	M	M	M	L	L	L	7	6	7	5	6	6	6	5	5	5
R16	T41	V34	1	3	H	M	H	L	H	H	M	L	L	L	5	4	5	3	5	5	4	3	3	3

Continued on next page

Table 5.10: continued from previous page

					Impact (Asset)			Impact (Goal)							AII			GII						
ID	Threat	Vulnerability	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical
R17	T92	V34	1	3	M	H	H	L	L	M	L	L	L	M	4	5	5	3	3	4	3	3	3	4
R18	T69	V43	3	3	M	H	H	M	L	L	L	M	L	M	6	7	7	6	5	5	5	6	5	6
R19	T24	V87	4	3	H	H	M	L	M	H	L	M	L	L	8	8	7	6	7	8	6	7	6	6
R20	T88	V66	1	2	L	M	H	M	M	L	L	L	L	H	2	3	4	3	3	2	2	2	2	4
R21	T73	V83	2	2	H	M	M	L	M	L	M	L	L	M	5	4	4	3	4	3	4	3	3	4
R22	T39	V40	1	1	L	L	H	L	L	L	M	L	L	L	1	1	3	1	1	1	2	1	1	1
R23	T18	V4	2	3	M	H	H	L	M	L	L	M	L	H	5	6	6	4	5	4	4	5	4	6
R24	T40	V17	1	2	M	H	H	L	L	L	L	M	L	H	3	4	4	2	2	2	2	3	2	4
R25	T45	V84	1	1	M	H	M	H	H	M	L	M	L	M	2	3	2	3	3	2	1	2	1	2
R26	T71	V28	4	3	H	M	M	M	L	L	L	M	L	M	8	7	7	7	6	6	6	7	6	7
R27	T74	V5	1	3	M	H	M	L	L	M	L	L	L	M	4	5	4	3	3	4	3	3	3	4
R28	T28	V92	4	4	H	M	M	L	M	M	M	H	M	H	9	8	8	7	8	8	8	9	8	9
R29	T66	V24	2	4	H	H	M	H	M	L	L	M	L	H	7	7	6	7	6	5	5	6	5	7
R30	T61	V99	1	2	M	M	M	L	M	M	L	M	L	M	3	3	3	2	3	3	2	3	2	3

Risk Determination

The participants determined the level of risk for each asset and goal using the formulas provided in Section 4.4.4. The values for the three elements of assets and seven elements of the goals calculated to determine the total sum for Asset Risk Indicator (ARI) and Goal Risk Indicator (GRI). The calculation for each risk is presented in Table 5.11, which sets out columns showing the total level for risk to assets and goals. The risks are colour-coded to present the category for each determined risk better; the colour of green is very low, yellow is low, orange is medium and high is red.

Following the example discussed in the previous view, the assessment of impacts to asset and goals in risk scenario (R8) results in AII{8,7,8} and GII{7,6,7,6,7,6,7}. The determination of the risk results in ARI{23} and GRI{46}. For a better presentation of the risks during the modelling process, each ARI and GRI represented as Risk ID{ARI,GRI}, e.g., R8{23,46}.

Table 5.11: Risk determination - AHC

					Impact (Asset)			**Impact (Goal)**							**AII**			**GII**							**Risk**	
ID	Threat	Vulnerability	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	ARI	GRI
R1	T100	V60	1	4	L	M	H	M	L	L	M	L	L	M	4	5	6	5	4	4	5	4	4	5	15	31
R2	T94	V13	2	3	H	M	M	L	L	L	L	M	L	H	6	5	5	4	4	4	4	5	4	6	16	31
R3	T5	V35	2	1	L	H	H	M	M	M	M	L	L	M	2	4	4	3	3	3	3	2	2	3	10	19
R4	T10	V87	2	3	H	H	M	M	M	H	L	H	L	M	6	6	5	5	5	6	4	6	4	5	17	35
R5	T70	V91	1	2	H	H	M	L	H	M	L	H	L	M	4	4	3	2	4	3	2	4	2	3	11	20
R6	T74	V36	1	2	H	H	M	L	L	M	L	M	L	M	4	4	3	2	2	3	2	3	2	3	11	17
R7	T45	V16	1	2	M	H	M	M	L	L	L	L	L	L	3	4	3	3	2	2	2	2	2	2	10	15
R8	T65	V44	3	4	H	M	H	M	L	M	L	M	L	M	8	7	8	7	6	7	6	7	6	7	23	46
R9	T5	V45	1	1	M	M	M	L	L	M	L	L	L	M	2	2	2	1	1	2	1	1	1	2	6	9
R10	T76	V64	3	3	M	M	M	M	H	M	L	L	L	M	6	6	6	6	7	6	5	5	5	6	18	40
R11	T56	V7	2	2	M	H	H	M	L	M	L	M	L	M	4	5	5	4	3	4	3	4	3	4	14	25
R12	T50	V24	3	3	M	H	H	M	M	H	L	H	L	M	6	7	7	6	6	7	5	7	5	6	20	42
R13	T10	V47	3	4	H	H	M	L	H	M	L	M	L	M	8	8	7	6	8	7	6	7	6	7	23	47
R14	T54	V92	1	3	H	H	M	L	M	M	L	H	L	M	5	5	4	3	4	4	3	5	3	4	14	26
R15	T56	V71	3	3	H	M	H	L	M	M	M	L	L	L	7	6	7	5	6	6	6	5	5	5	20	38
R16	T41	V34	1	3	H	M	H	L	H	H	M	L	L	L	5	4	5	3	5	5	4	3	3	3	14	26
R17	T92	V34	1	3	M	H	H	L	L	M	L	L	L	M	4	5	5	3	3	4	3	3	3	4	14	23
R18	T69	V43	3	3	M	H	H	M	L	L	L	M	L	M	6	7	7	6	5	5	5	6	5	6	20	38
R19	T24	V87	4	3	H	H	M	L	M	H	L	M	L	L	8	8	7	6	7	8	6	7	6	6	23	46
R20	T88	V66	1	2	L	M	H	M	M	L	L	L	L	H	2	3	4	3	3	2	2	2	2	4	9	18
R21	T73	V83	2	2	H	M	M	L	M	L	M	L	L	M	5	4	4	3	4	3	4	3	3	4	13	24
R22	T39	V40	1	1	L	L	H	L	L	L	M	L	L	L	1	1	3	1	1	1	2	1	1	1	5	8
R23	T18	V4	2	3	M	H	H	L	M	L	L	M	L	H	5	6	6	4	5	4	4	5	4	6	17	32
R24	T40	V17	1	2	M	H	H	L	L	L	L	M	L	H	3	4	4	2	2	2	2	3	2	4	11	17
R25	T45	V84	1	1	M	H	M	H	H	M	L	M	L	M	2	3	2	3	3	2	1	2	1	2	7	14
R26	T71	V28	4	3	H	M	M	M	L	L	L	M	L	M	8	7	7	7	6	6	6	7	6	7	22	45
R27	T74	V5	1	3	M	H	M	L	L	M	L	L	L	M	4	5	4	3	3	4	3	3	3	4	13	23
R28	T28	V92	4	4	H	M	M	L	M	M	M	H	M	H	9	8	8	7	8	8	8	9	8	9	25	57
R29	T66	V24	2	4	H	H	M	H	M	L	L	M	L	H	7	7	6	7	6	5	5	6	5	7	20	41
R30	T61	V99	1	2	M	M	M	L	M	M	L	M	L	M	3	3	3	2	3	3	2	3	2	3	9	18

Risk Evaluation

AHC adopted the evaluation method for evaluating the results of the risk assessment. The acceptance criteria in Table 4.8 used for decision making and evaluating the ARI. Similarly, the acceptance criteria in Table 4.9 used for evaluating the GRI.

Following the example discussed in the previous view, the determination of ARI and GRI in risk scenario (R8) evaluated accordingly. The ARI value of (23) is within the category of 22-27 defined as High, meaning that "Action must be taken to reduce the risk". The GRI value of (46) is within the category of 32-47 defined as Medium, meaning that "Action should be taken to reduce the risk. The top management may accept".

Risk Treatment

AHC decided to treat all risks using mitigation approach by introducing necessary controls rather than to avoid or transfer the risks. Table 5.12 describes the risk treatment control selected from the Annex A of the ISO/IEC 27001:2013 for each identified risk scenario. It assigns a unique ID to each control followed by the description summary of the treatment.

The columns in the left part of the table include a risk identifier matching the risk scenario, and values for the likelihoods, ease of exploits, ARI and GRI prior to treatment of the risks. On the other hand, the columns on the right part of the table show the residual values upon successful implementation of the controls. It provides new values following the reassessment of the likelihoods and ease of exploits, however, the level of consequences to the elements of the assets and goals remained the same since the nature of the threats and vulnerabilities have not changed. Next, the residual values used to recalculate using the risk matrix in Table 4.7.

Following the example discussed in the previous view, the treatment of the risk scenario (R8) was treated by introducing a treatment control (TC74) defines as "controls against malware". The reassessed level of the threat's (T65) likelihood established as low (2) and the vulnerability's (V44) ease of exploit as low (2). The reassessed calculation of the impact to each element of the asset determined value for the confidentiality is (5), integrity is (4), and availability is (5). The recalculation of the GII determined the indicator value for the business is (4), financial is (3), legal is (4), physical is (3), privacy is (4), social is (3) and technical is (4). The residual risks result in ARI{14} and GRI{25}.

Again, for a better presentation of the residual risks during the modelling process, each residual ARI and GRI are represented as Risk ID{ARI,GRI}, e.g., R8{14,25}. A Statement of Applicability produced and provided in Appendix C.

Table 5.12: Risk treatment - AHC

					Risk		Residual														
									AII			GII								Risk	
ID	Description	Risk	Likelihood	Ease of exploit	ARI	GRI	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	ARI	GRI
TC131	Securing offices, rooms and facilities	R1	1	4	15	31	1	2	2	3	4	3	2	2	3	2	2	3	9	17
TC95	Physical entry controls	R2	2	3	16	31	1	1	3	2	2	1	1	1	1	2	1	3	7	10
TC50	Information security continuity	R3	2	1	10	19	1	1	1	3	3	2	2	2	2	1	1	2	7	12
TC62	Information transfer policies	R4	2	3	17	35	1	2	4	4	3	3	3	4	2	4	2	3	11	21
TC2	Access control policy	R5	1	2	11	20	1	2	4	4	3	2	4	3	2	4	2	3	11	20
TC37	Disposal of media	R6	1	2	11	17	1	1	3	3	2	1	1	2	1	2	1	2	8	10
TC58	Information security policy for supplier relationships	R7	1	2	10	15	1	1	2	3	2	2	1	1	1	1	1	1	7	8
TC74	Controls against malware	R8	3	4	23	46	2	2	5	4	5	4	3	4	3	4	3	4	14	25
TC0	Accept	R9	1	1	6	9	1	1	2	2	2	1	1	2	1	1	1	2	6	9
TC154	Use of secret authentication information	R10	3	3	18	40	2	1	3	3	3	3	4	3	2	2	2	3	9	19
TC18	Capacity management	R11	2	2	14	25	2	1	3	4	4	3	2	3	2	3	2	3	11	18
TC135	Security training	R12	3	3	20	42	2	1	3	4	4	3	3	4	2	4	2	3	11	21
TC22	Clear desk and clear screen policy	R13	3	4	23	47	2	2	5	5	4	3	5	4	3	4	3	4	14	26
TC86	Network controls	R14	1	3	14	26	1	2	4	4	3	2	3	3	2	4	2	3	11	19
TC38	Documented operating procedures	R15	3	3	20	38	2	2	5	4	5	3	4	4	4	3	3	3	14	24
TC45	Event logging	R16	1	3	14	26	1	2	4	3	4	2	4	4	3	2	2	2	11	19
TC145	System change control procedures	R17	1	3	14	23	1	2	3	4	4	2	2	3	2	2	2	3	11	16
TC2	Access control policy	R18	3	3	20	38	2	2	4	5	5	4	3	3	3	4	3	4	14	24

Continued on next page

Table 5.12: continued from previous page

					Risk		Residual														
									AII			GII								Risk	
ID	Description	Risk	Likelihood	Ease of exploit	ARI	GRI	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	ARI	GRI
TC62	Information transfer policies	R19	4	3	23	46	2	2	5	5	4	3	4	5	3	4	3	3	14	25
TC98	Planning security continuity	R20	1	2	9	18	1	1	1	2	3	2	2	1	1	1	1	3	6	11
TC143	Surge protector	R21	2	2	13	24	1	1	3	2	2	1	2	1	2	1	1	2	7	10
TC0	Accept	R22	1	1	5	8	1	1	1	1	3	1	1	1	2	1	1	1	5	8
TC92	Password management system	R23	2	3	17	32	1	2	3	4	4	2	3	2	2	3	2	4	11	18
TC104	Protecting services transactions	R24	1	2	11	17	1	1	2	3	3	1	1	1	1	2	1	3	8	10
TC0	Accept	R25	1	1	7	14	1	1	2	3	2	3	3	2	1	2	1	2	7	14
TC38	Documented operating procedures	R26	4	3	22	45	3	2	6	5	5	5	4	4	4	5	4	5	16	31
TC37	Disposal of media	R27	1	3	13	23	1	1	2	3	2	1	1	2	1	1	1	2	7	9
TC14	Boundary defence	R28	4	4	25	57	2	2	5	4	4	3	4	4	4	5	4	5	13	29
TC38	Documented operating procedures	R29	2	4	20	41	2	2	5	5	4	5	4	3	3	4	3	5	14	27
TC45	Event logging	R30	1	2	9	18	1	1	2	2	2	1	2	2	1	2	1	2	6	11

Risk Acceptance

AHC evaluated the residual results of the ARI and GRI using the same method and the evaluation criteria discussed in Section 4.4.5. AHC noted that all residual risks met the organisation risk acceptance criteria and the risk owners approved the level of residual risks, hence, no further adjustment or risk treatment required at this stage. The full results of the information security risk management are presented in Table 5.13.

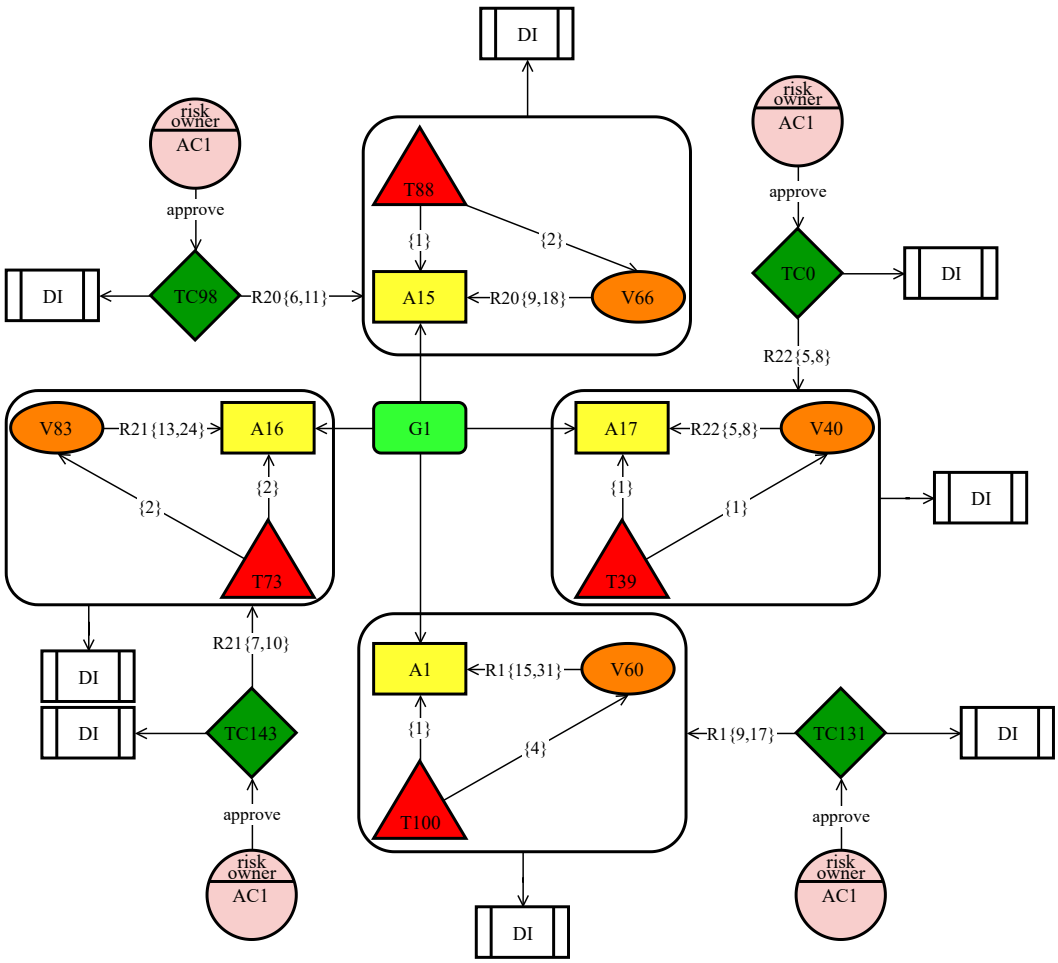
Table 5.13: Overview of the information security risk management - AHC

							Impact (Asset)			**Impact (Goal)**							**AII**			**GII**							**Risk**			**Residual**															
																															AII			**GII**							**Risk**		
ID	Goal	Asset	Threat	Vulnerability	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	ARI	GRI	Treatment	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	ARI	GRI
R1	G1	A1	T100	V60	1	4	L	M	H	M	L	L	M	L	L	M	4	5	6	5	4	4	5	4	4	5	15	31	TC131	1	2	2	3	4	3	2	2	3	2	2	3	9	17
R2	G2	A2	T94	V13	2	3	H	M	M	L	L	L	L	M	L	H	6	5	5	4	4	4	4	5	4	6	16	31	TC95	1	1	3	2	2	1	1	1	1	2	1	3	7	10
R3	G3	A3	T5	V35	2	1	L	H	H	M	M	M	M	L	L	M	2	4	4	3	3	3	3	2	2	3	10	19	TC50	1	1	1	3	3	2	2	2	2	1	1	2	7	12
R4	G4	A4	T10	V87	2	3	H	H	M	M	M	H	L	H	L	M	6	6	5	5	5	6	4	6	4	5	17	35	TC62	1	2	4	4	3	3	3	4	2	4	2	3	11	21
R5	G4	A4	T70	V91	1	2	H	H	M	L	H	M	L	H	L	M	4	4	3	2	4	3	2	4	2	3	11	20	TC2	1	2	4	4	3	2	4	3	2	4	2	3	11	20
R6	G5	A6	T74	V36	1	2	H	H	M	L	L	M	L	M	L	M	4	4	3	2	2	3	2	3	2	3	11	17	TC37	1	1	3	3	2	1	1	2	1	2	1	2	8	10
R7	G5	A6	T45	V16	1	2	M	H	M	M	L	L	L	L	L	L	3	4	3	3	2	2	2	2	2	2	10	15	TC58	1	1	2	3	2	2	1	1	1	1	1	1	7	8
R8	G20	A12	T65	V44	3	4	H	M	H	M	L	M	L	M	L	M	8	7	8	7	6	7	6	7	6	7	23	46	TC74	2	2	5	4	5	4	3	4	3	4	3	4	14	25
R9	G24	A6	T5	V45	1	1	M	M	M	L	L	M	L	L	L	M	2	2	2	1	1	2	1	1	1	2	6	9	TC0	1	1	2	2	2	1	1	2	1	1	1	2	6	9
R10	G24	A6	T76	V64	3	3	M	M	M	M	H	M	L	L	L	M	6	6	6	6	7	6	5	5	5	6	18	40	TC154	2	1	3	3	3	3	4	3	2	2	2	3	9	19
R11	G10	A14	T56	V7	2	2	M	H	H	M	L	M	L	M	L	M	4	5	5	4	3	4	3	4	3	4	14	25	TC18	2	1	3	4	4	3	2	3	2	3	2	3	11	18
R12	G11	A14	T50	V24	3	3	M	H	H	M	M	H	L	H	L	M	6	7	7	6	6	7	5	7	5	6	20	42	TC135	2	1	3	4	4	3	3	4	2	4	2	3	11	21
R13	G14	A10	T10	V47	3	4	H	H	M	L	H	M	L	M	L	M	8	8	7	6	8	7	6	7	6	7	23	47	TC22	2	2	5	5	4	3	5	4	3	4	3	4	14	26
R14	G15	A10	T54	V92	1	3	H	H	M	L	M	M	L	H	L	M	5	5	4	3	4	4	3	5	3	4	14	26	TC86	1	2	4	4	3	2	3	3	2	4	2	3	11	19
R15	G26	A13	T56	V71	3	3	H	M	H	L	M	M	M	L	L	L	7	6	7	5	6	6	6	5	5	5	20	38	TC38	2	2	5	4	5	3	4	4	4	3	3	3	14	24

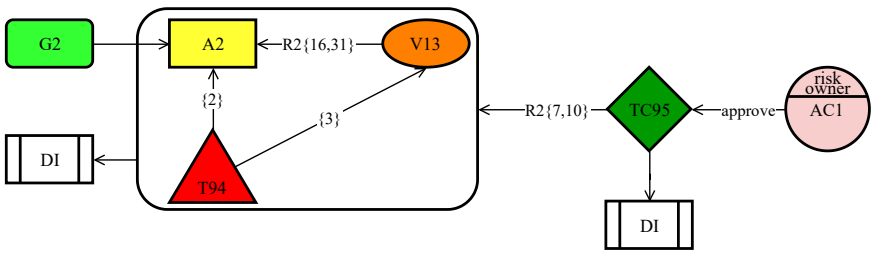
Continued on next page

Table 5.13: continued from previous page

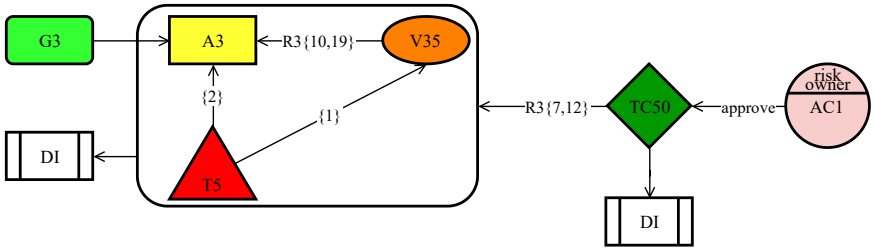
							Impact (Asset)			**Impact (Goal)**							**AII**			**GII**							**Risk**			**Residual**														
																															AII			**GII**							**Risk**		
ID	Goal	Asset	Threat	Vulnerability	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	ARI	GRI	Treatment	Likelihood	Ease of exploit	Confidentiality	Integrity	Availability	Business	Financial	Legal	Physical	Privacy	Social	Technical	ARI	GRI
R16	G27	A13	T41	V34	1	3	H	M	H	L	H	H	M	L	L	L	5	4	5	3	5	5	4	3	3	3	14	26	TC45	1	2	4	3	4	2	4	4	3	2	2	2	11	19
R17	G5	A14	T92	V34	1	3	M	H	H	L	L	M	L	L	L	M	4	5	5	3	3	4	3	3	3	4	14	23	TC145	1	2	3	4	4	2	2	3	2	2	2	3	11	16
R18	G5	A14	T69	V43	3	3	M	H	H	M	L	L	L	M	L	M	6	7	7	6	5	5	5	6	5	6	20	38	TC2	2	2	4	5	5	4	3	3	3	4	3	4	14	24
R19	G5	A11	T24	V87	4	3	H	H	M	L	M	H	L	M	L	L	8	8	7	6	7	8	6	7	6	6	23	46	TC62	2	2	5	5	4	3	4	5	3	4	3	3	14	25
R20	G1	A15	T88	V66	1	2	L	M	H	M	M	L	L	L	L	H	2	3	4	3	3	2	2	2	2	4	9	18	TC98	1	1	1	2	3	2	2	1	1	1	1	3	6	11
R21	G1	A16	T73	V83	2	2	H	M	M	L	M	L	M	L	L	M	5	4	4	3	4	3	4	3	3	4	13	24	TC143	1	1	3	2	2	1	2	1	2	1	1	2	7	10
R22	G1	A17	T39	V40	1	1	L	L	H	L	L	L	M	L	L	L	1	1	3	1	1	1	2	1	1	1	5	8	TC0	1	1	1	1	3	1	1	1	2	1	1	1	5	8
R23	G6	A18	T18	V4	2	3	M	H	H	L	M	L	L	M	L	H	5	6	6	4	5	4	4	5	4	6	17	32	TC92	1	2	3	4	4	2	3	2	2	3	2	4	11	18
R24	G9	A18	T40	V17	1	2	M	H	H	L	L	L	L	M	L	H	3	4	4	2	2	2	2	3	2	4	11	17	TC104	1	1	2	3	3	1	1	1	1	2	1	3	8	10
R25	G6	A19	T45	V84	1	1	M	H	M	H	H	M	L	M	L	M	2	3	2	3	3	2	1	2	1	2	7	14	TC0	1	1	2	3	2	3	3	2	1	2	1	2	7	14
R26	G6	A19	T71	V28	4	3	H	M	M	M	L	L	L	M	L	M	8	7	7	7	6	6	6	7	6	7	22	45	TC38	3	2	6	5	5	5	4	4	4	5	4	5	16	31
R27	G5	A5	T74	V5	1	3	M	H	M	L	L	M	L	L	L	M	4	5	4	3	3	4	3	3	3	4	13	23	TC37	1	1	2	3	2	1	1	2	1	1	1	2	7	9
R28	G9	A18	T28	V92	4	4	H	M	M	L	M	M	M	H	M	H	9	8	8	7	8	8	8	9	8	9	25	57	TC14	2	2	5	4	4	3	4	4	4	5	4	5	13	29
R29	G19	A23	T66	V24	2	4	H	H	M	H	M	L	L	M	L	H	7	7	6	7	6	5	5	6	5	7	20	41	TC38	2	2	5	5	4	5	4	3	3	4	3	5	14	27
R30	G12	A26	T61	V99	1	2	M	M	M	L	M	M	L	M	L	M	3	3	3	2	3	3	2	3	2	3	9	18	TC45	1	1	2	2	2	1	2	2	1	2	1	2	6	11



(a) Goal category: Provide secure trading environment

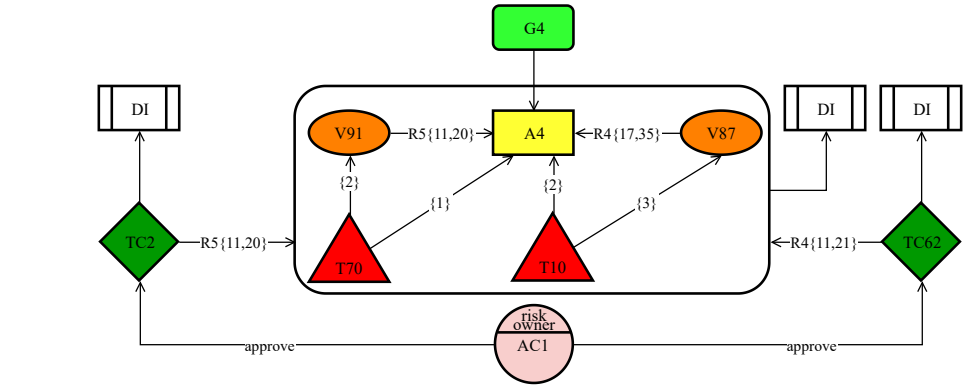


(b) Goal category: Minimise litigation

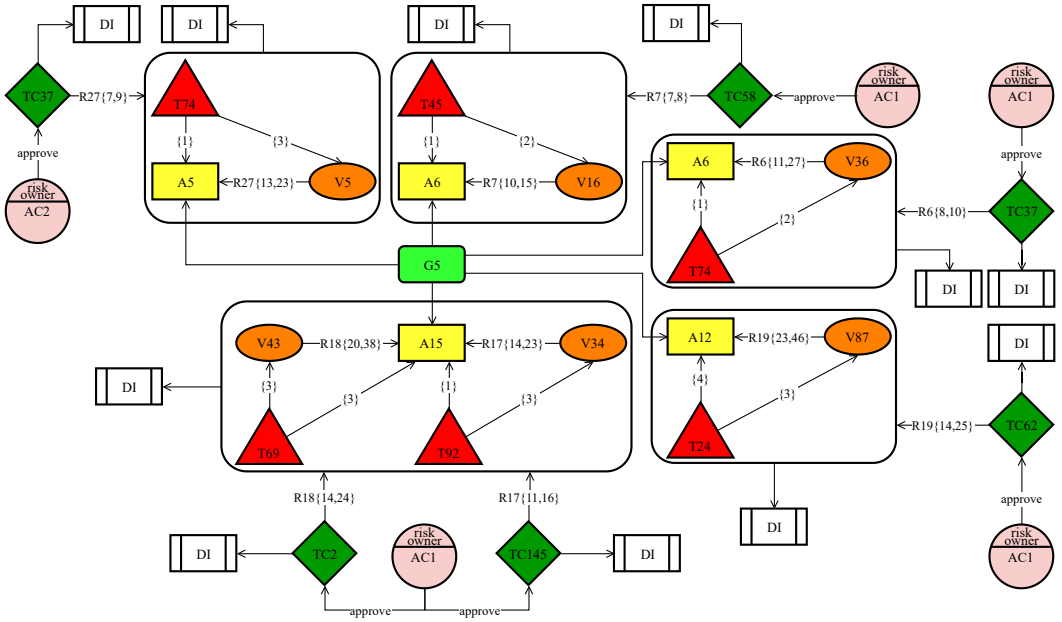


(c) Goal category: Competitive advantage

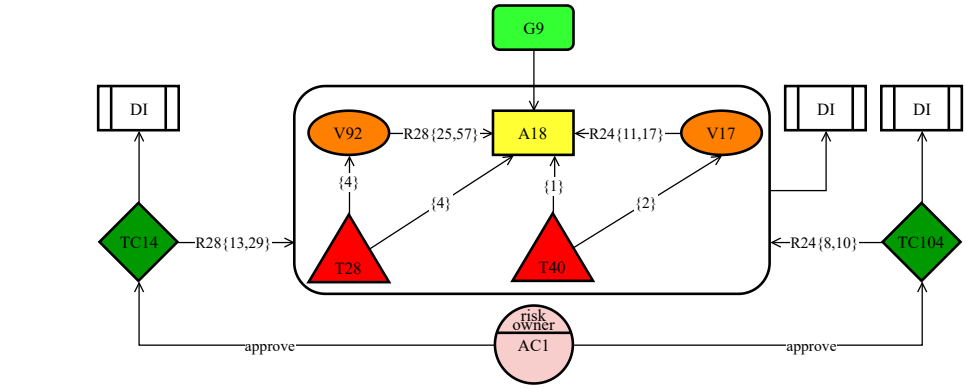
Figure 5.3: Technical Viewpoint - AHC



(d) Goal category: Protect trade secret

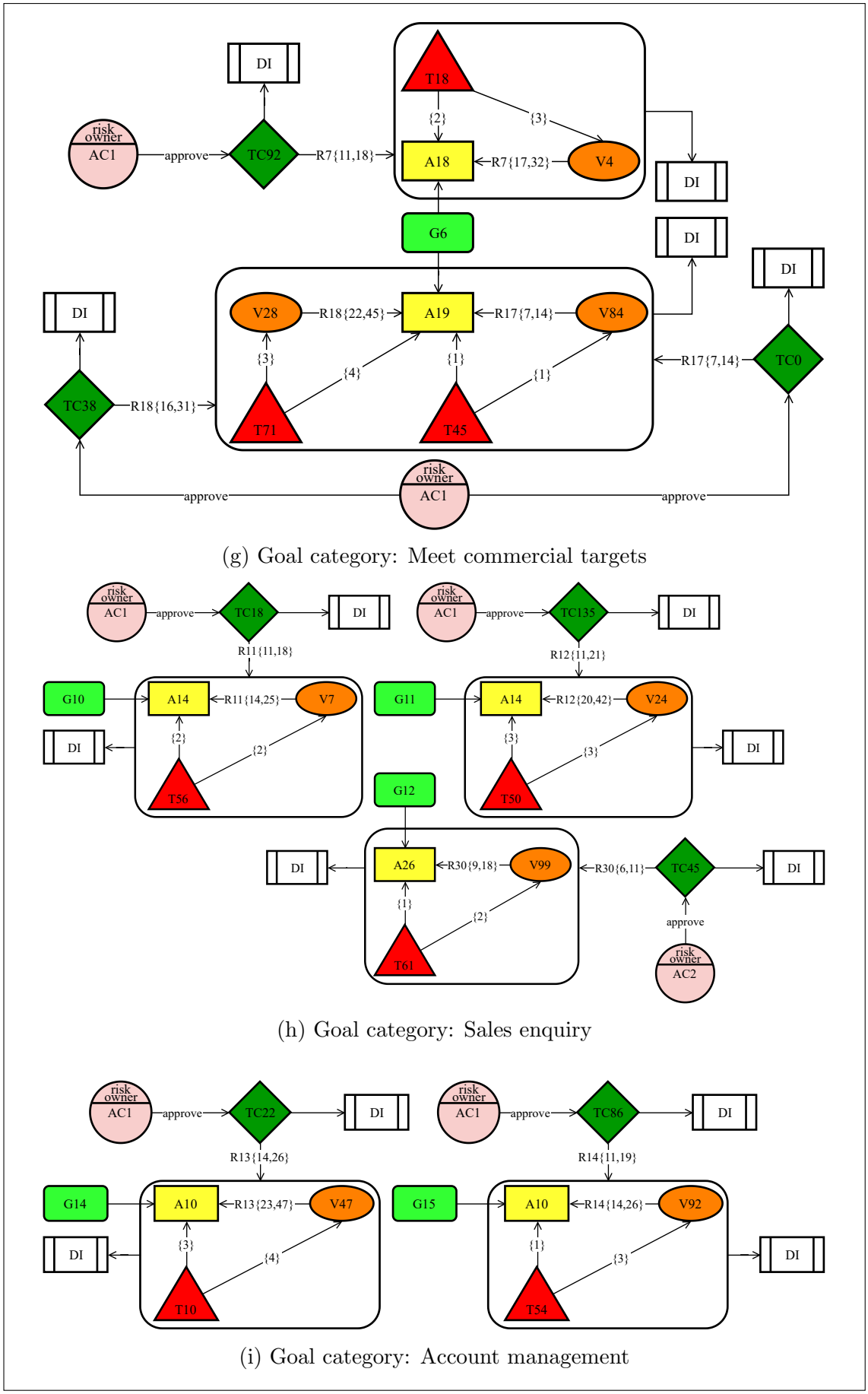


(e) Goal category: Support legal and regulatory compliance



(f) Goal category: Contact enquiry

Figure 5.3: Technical Viewpoint (cont.)

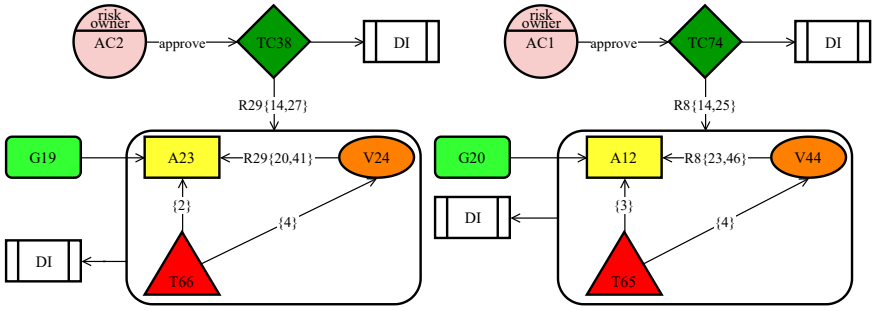


(g) Goal category: Meet commercial targets

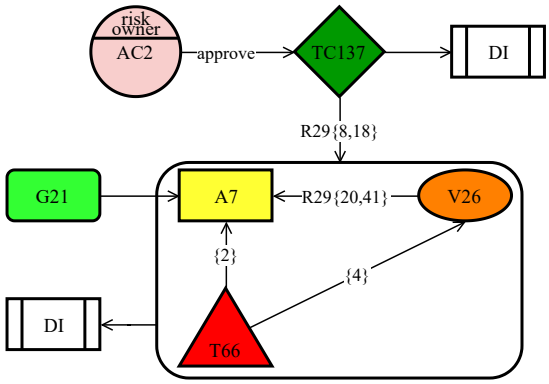
(h) Goal category: Sales enquiry

(i) Goal category: Account management

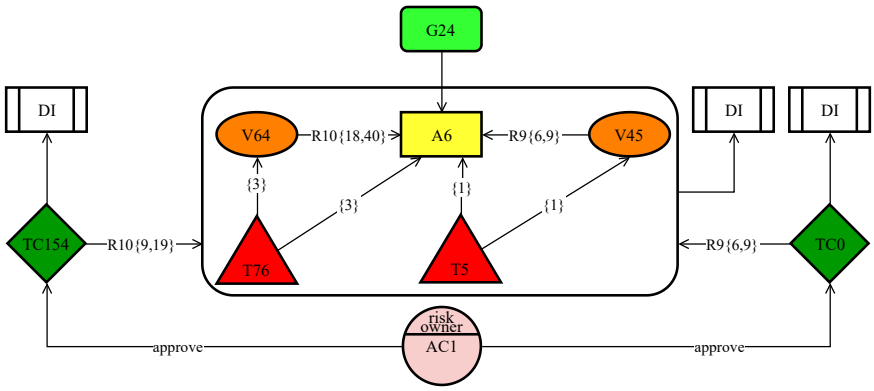
Figure 5.3: Technical Viewpoint (cont.)



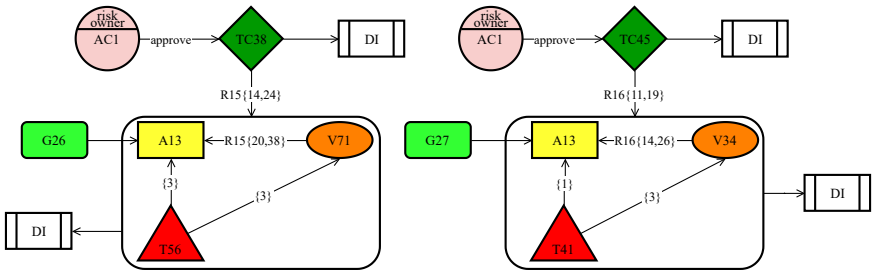
(j) Goal category: Quote opening



(k) Goal category: Payment



(l) Goal category: Contracts



(m) Goal category: Claim management

Figure 5.3: Technical Viewpoint

5.3.4 System Viewpoint

In the same vein, the System Viewpoint required a conjunction input from various stakeholders in the AHC. The Objectives Specification View in this viewpoint involved selection of contributions that required expert directions provided by the AHC member of the IT team and business advisor. The following two sections describe the implementation of the views in the System Viewpoint.

While modelling of the roles have dispersed in the overall parts of INFORMS, the modelling of the information security objectives are shown in Figure 5.4.

Roles Identification

The top management played an active role in assigning roles and deciding the responsibilities for each mandatory role. AHC identified and assigned several actors across the five roles proposed by INFORMS. Table 5.14 summarises the responsibilities of each actor related to the ISMS for all five roles. The roles and responsibilities assigned and adjusted as necessary during the modelling of each viewpoint.

Some actors like Office Manager (AC2) associates with more than one role, while most identified actors are responsible for one role, e.g., custodian.

There is no guideline for selecting roles to collect and review information in activities such as monitoring and measurement. However, roles such as collector and reviewer should hold the necessary competency in the assigned activities. AHC decided to appoint a member of IT contractor (AC13) to collect and review the processes related to information security along with a member of the top management to monitor and review other operational activities in the organisation.

Table 5.14: Description of roles - AHC

Actor	**Risk owner**	**Custodian**	**Collector**	**Reviewer**	**Internal Auditor**
AC1	+				
AC2	+		+	+	
AC6		+			
AC7		+			
AC8		+			
AC9		+			
AC10		+			
AC11		+			
AC12		+			+
AC13		+	+	+	+

Objectives Specification

The top management identified the information security objectives with the support of a member of the IT contractor as required. AHC emphasises on the confidentiality of information assets, availability of the business operation and consideration to avoid any potential attacks or data breaches of their customer's sensitive information, e.g., a ransomware attack. The top management chose seven information security objectives for the ISMS, as shown in Table 5.15.

The participants decided that a representative of the top management is a suitable candidate for taking responsibility in managing the achievement of the objectives as well as monitoring to ensure the necessary progress is in place to achieve the completion target value.

For example, the first objective (O1) describes the "number of employees receive security training" to address a requirement of the ISMS that expects actors doing work under its control to be aware of their contribution to the effectiveness of the ISMS. O1 satisfies the requirement of the constraint (C20) introduced by the Financial Conduct Authority (AC18), who requires the organisation's internal actors to receive sufficient "training and awareness" related to information security.

The resources identified as available to fulfil the objective are information security treatment controls (TC79) and (TC135), which both indicates that the management should take the responsibility of assessing the security skills of the internal actors and plan the appropriate training to fill the gaps.

The target value given to assess the successful completion of the objective is 100%; this expects the organisation to provide a necessary information security training and awareness to all relevant actors, i.e., this objective applies to 100% of actors.

The evaluation for the achievement of the objective is quarterly, AHC has three months from the specification of the objective to achieve the target value of the objective.

Table 5.15: Information security objectives - AHC

ID	Description	Role	Constraint	Resource	Target	Completion
O1	Number of employees receive information security training	AC2	C20	TC135	=100%	Quarterly
O2	Impact on assets due to inappropriate level of protection responsibilities	AC2	C6, C7, C8, C9, C10, C11, C15	TC2, TC74, TC154	=95%	Yearly
O3	Number of insecure access to information assets	AC13	C3, C5, C12, C13, C14	TC2, TC37, TC92	<=2	Semester
O4	Full back up failures	AC13	C21	TC45, TC54, TC131, TC143	<=2	Semester
O5	Count of information disclosure due to poor communication security	AC13	C1, C2	TC14, TC58, TC62, TC86, TC104, TC145	=100%	Semester
O6	Legal issues	AC1	C4, C16, C17, C18, C19	TC18, TC38	=100%	Yearly
O7	Downtime due to lack of business continuity	AC2	-	TC50, TC98	<=1	Yearly

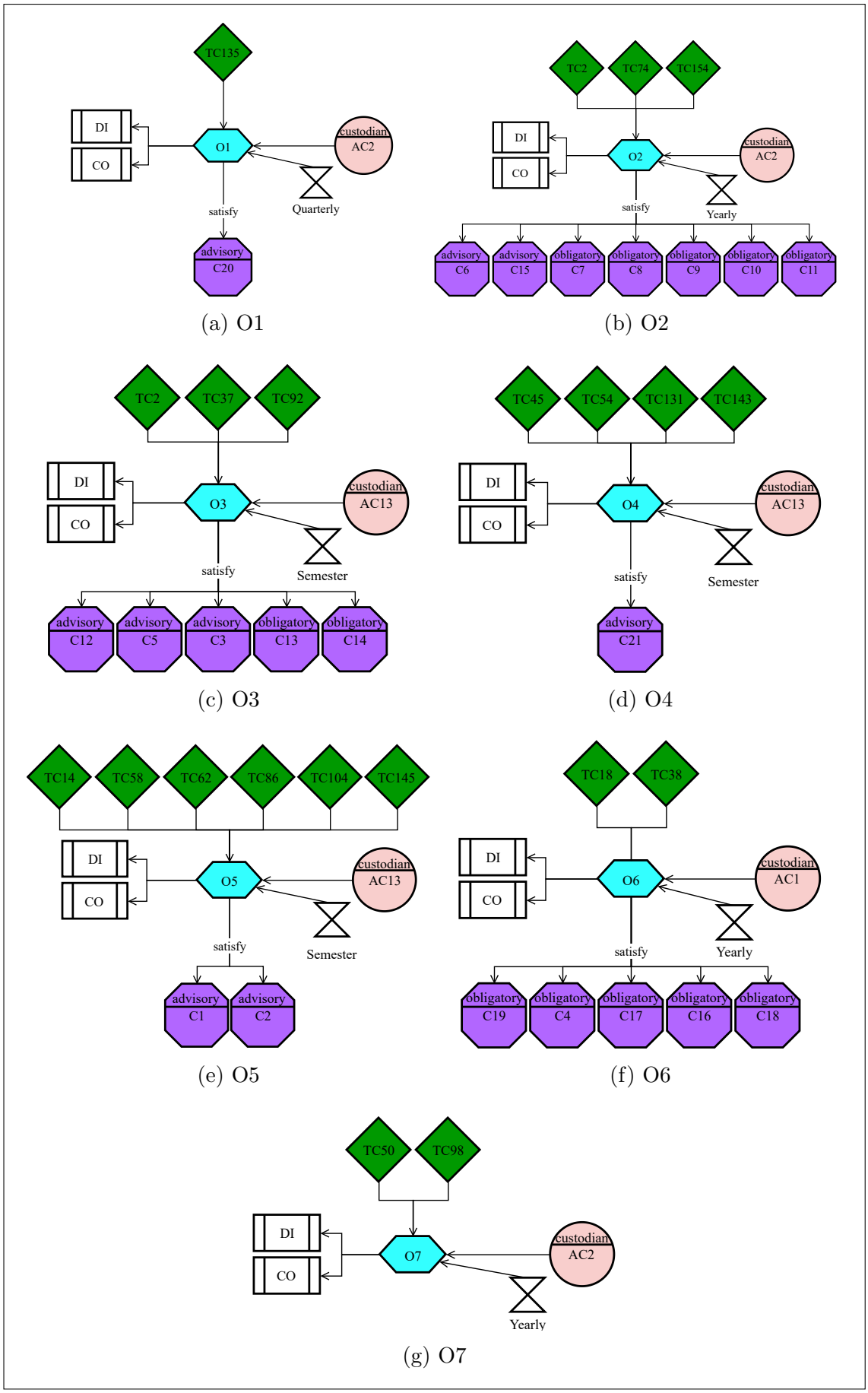


Figure 5.4: Objectives Specification View - AHC

5.3.5 Standard Viewpoint

The Standard Viewpoint was the final viewpoint in the application of the INFORMS framework in the implementation of the ISMS in the AHC. The following five sections describe the implementation of the views in this viewpoint.

Monitoring and Measurement

AHC determined number of information security controls and processes to monitor, measure, analyse and evaluate the effectiveness of the ISMS. AHC had to monitor the functioning of the information security processes and controls as required by the operation of the organisation; it measured their conformity with the ISMS including the satisfaction of the constraints by the actors.

In order to achieve the above, the organisation modelled seven processes to monitor and their effectiveness to be measured, as shown in Figure 5.5. AHC evaluated the result of the monitoring and measurement against the established baselines, which enabled the organisation to protect the information assets and reduce future risks proactively.

Table 5.16 describes the selected security processes and controls on the advice of the Office Manager (AC2) and a member of the IT contractor (AC13).

The table provides a monitoring and measurement ID for a particular process or control, followed by a short description of what is required to be monitored and measured. The Process/Control column indicates what process or control is specifically monitored and measured. The interval (collect) indicates the frequency of the monitoring and measurement to be collected on the identified processes and controls, while the interval (review) indicates the frequency of when the result of the monitoring and measurement should be reviewed. The table provides the two roles involved in collecting and reviewing monitoring and measurement processes and controls.

For example, AHC decided to monitor and measure "physical entry controls effectiveness" (MM4) to receive an assessment of the overall security of the physical entries. The controls involved are "clear screen and clear desk policy" (TC22), "physical entry controls" (TC95) and "securing offices, rooms and facilities" (TC131). All these controls need to monitor and measure by the Office Manager (AC2) every semester and the results to be reviewed by the same actor every semester too. The result of the MM4 should be recorded, documented and reported to the top management at the next Management Review meeting. Figure 5.5d models the MM4 using the INFORMS modelling language.

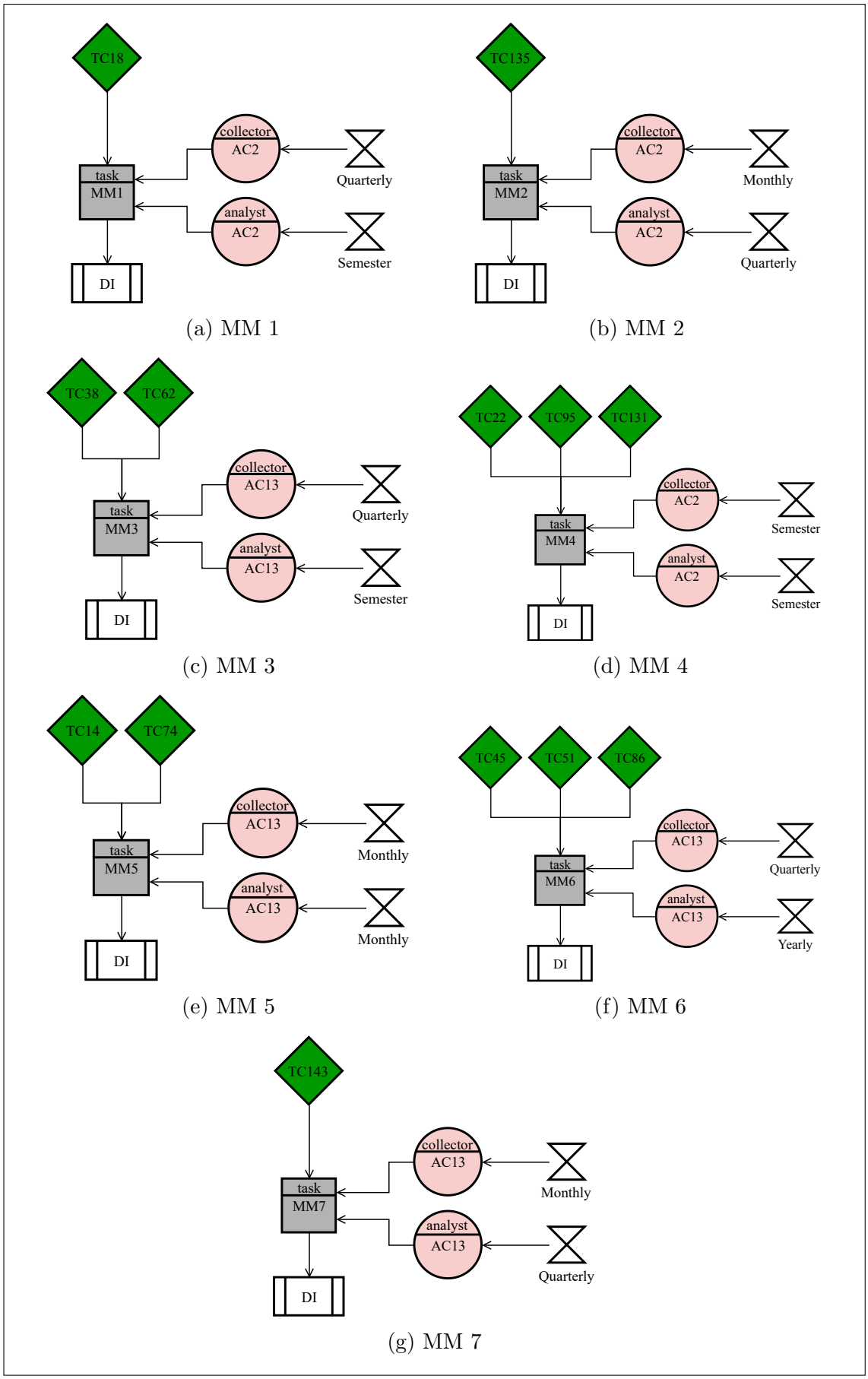


Figure 5.5: Monitoring and Measurement View - AHC

Table 5.16: Processes for monitoring and measurement - AHC

ID	Description	Process/ Control	Interval (collect)	Interval (review)	Role (collect)	Role (review)
MM1	Management commitment	TC18	Quarterly	Semester	AC2	AC2
MM2	ISMS training and awareness	TC135	Monthly	Quarterly	AC2	AC2
MM3	Social engineering preparedness	TC38, TC62	Quarterly	Semester	AC13	AC13
MM4	Physical entry controls effectiveness	TC22, TC95, TC131	Semester	Semester	AC2	AC2
MM5	Anti-malware	TC14, TC74	Monthly	Monthly	AC13	AC13
MM6	Security incident trend	TC45, TC86	Quarterly	Yearly	AC13	AC13
MM7	Device configuration	TC143	Monthly	Monthly	AC13	AC13

Internal Audit

AHC planned internal audit programme for the first year, the audit programme established to ensure the ISMS conforms to the organisation's requirements for the ISMS as well as the requirements of the standard. The organisation modelled seven plans as demonstrated in Figure 5.6, to be conducted at the planned interval.

Additionally, Table 5.17 describes the selected audit plans by a member of the top management and the implementer. The table provides an internal audit ID for a particular plan followed by a short description of the audit plan. All plans assigned with an internal auditor role, and the processes included for each audit mentioned in the scope of each audit plan. The interval for the audit indicates the scheduled time for the conduct of each audit plan.

For example, AHC planned to audit whether the "ISMS objectives are compatible with the strategic direction of the organisation" (IA1). To conduct the audit, a set of audit processes involved were "Number of employees receive information security training" (O1), "Impact on assets due to inappropriate level of protection responsibilities" (O2) and "Downtime due to lack of business continuity" (O7) to be conducted by the Office Manager (AC2) annually. The result of the IA1 should be recorded, documented and communicated to the top management. Figure 5.6a models the IA1 using the INFORMS modelling language.

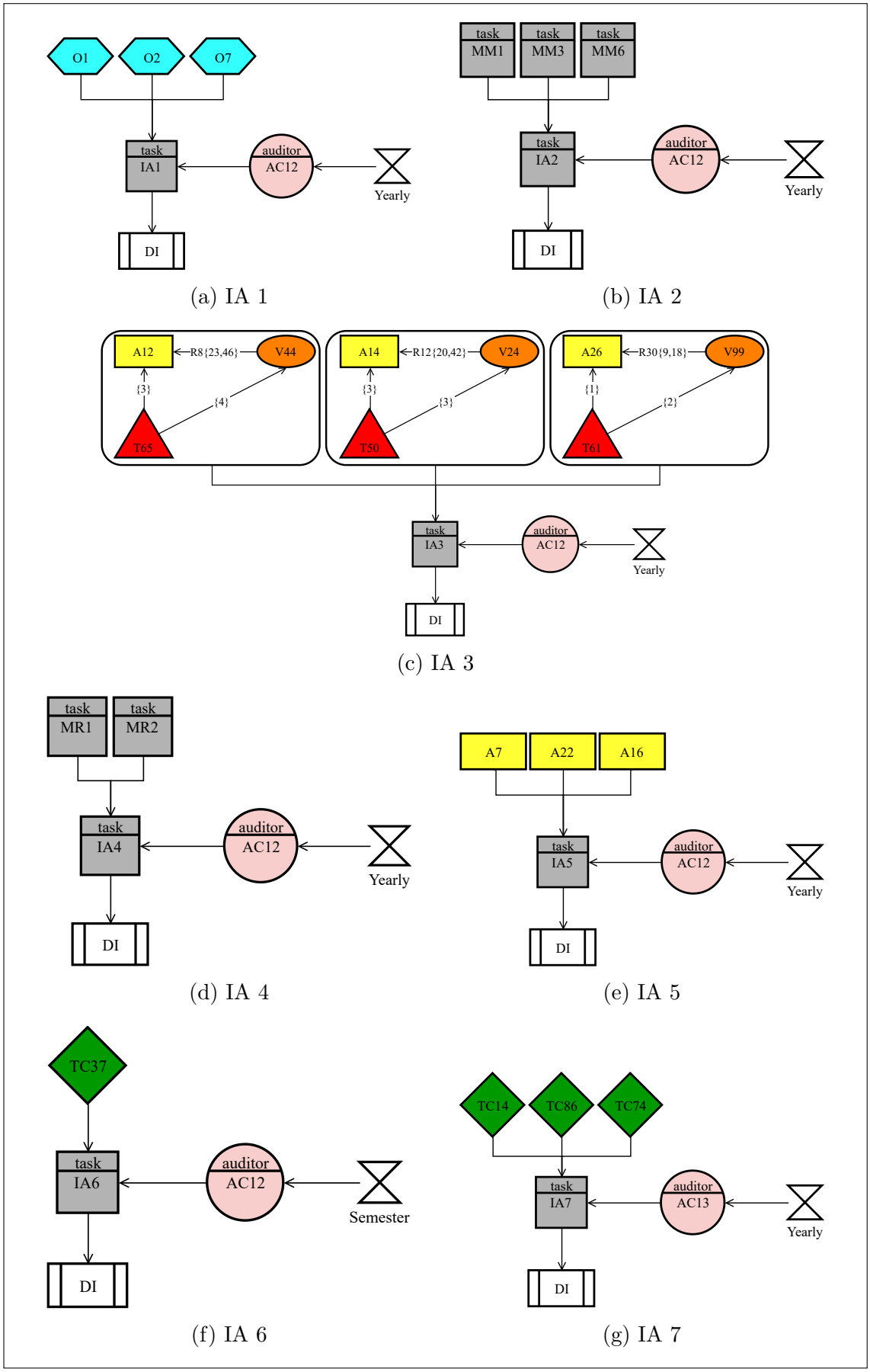


Figure 5.6: Internal Audit View - AHC

Table 5.17: Plans for the internal audit - AHC

ID	Description	Role	Process	Interval
IA1	Do the ISMS objectives compatible with the strategic direction of the organisation?	AC12	O1, O2, O7	Yearly
IA2	Do the monitoring and measurements activities defined and the method, responsible actor to evaluate the results identified?	AC12	MM1, MM3, MM6	Yearly
IA3	Do the results of the information security risks documented?	AC12	R8, R12, R30	Yearly
IA4	Do the top management identified all the crucial issues important for the success of the ISMS?	AC12	MR1, MR2	Yearly
IA5	Does every item in the inventory of assets have a designated owner?	AC12	A7, A16, A22	Yearly
IA6	Does a formal procedure exist for the dispose of the media?	AC12	TC37	Semester
IA7	Do anti-virus and other software for protection against malware installed and updated?	AC13	TC14, TC74, TC86	Yearly

Management Review

The management review of the AHC was at a very initial stage since the ISMS have implemented for a short period and the maturity of the ISMS could take up to a year before the top management has a chance to gather all the information from all activities in the ISMS and take them into consideration, e.g., the results of the Monitoring and Measurement View and Internal Audit View. AHC modelled two agenda for the management review as set out in Figure 5.7.

Table 5.18 describes the agenda in the management review. It indicates a unique ID number starting with MR1. Each management review needs to identify the processes for consideration in the reviews. The table lists the inputs required for the management review and also the interval of such a review. The outcome of the management reviews should include an identification of nonconformity(ies) if existed or suggestion for continual improvement.

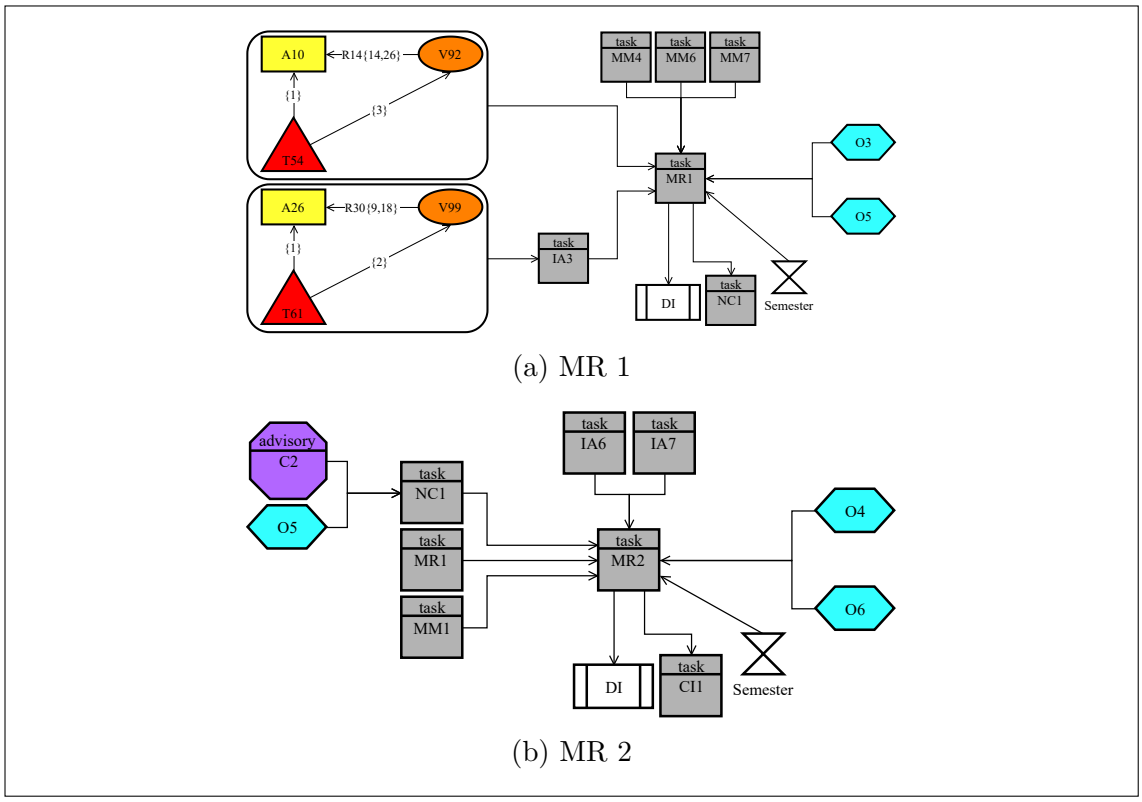
For example, MR1 happened in the first semester considered the MM4, MM6, MM7, R30, R14, O3 and O5. The result of the MR1 found one nonconformity (NC1). Figure 5.7a models the MR1 using the INFORMS modelling language. The result of the MR1 should be recorded and documented according to the procedures in the Documented Information View.

Nonconformity and Corrective Action

A nonconformity could occur at each part of the ISMS. AHC modelled one nonconformity and corrective action shown in Figure 5.8.

Table 5.18: Agenda for the management review - AHC

ID	Input	Interval	Outcome
MR1	O3, O5, MM4, MM6, MM7, IA3, R14, R30	Semester	NC1
MR2	O4, O6, MR1, MM1, IA6, IA7, NC1	Semester	CI1



(a) MR 1

(b) MR 2

Figure 5.7: Management Review View - AHC

Table 5.19 explains the nonconformity following the result of the management review (MR1). The source of the nonconformity was the number of information "disclosure due to poor communication security" (O5), which was not satisfied by the target value of the %100 as assigned in the previous semester, and as a result, a non-conformity (NC1) raised accordingly. The nonconformity could impact the objective (O2) and constraint (C2), a corrective action TC55 suggested to eliminate the root cause of the NC1.

Table 5.19: Register of the nonconformity and corrective action - AHC

ID	Cause	Impact	Corrective Action
NC1	Disclosure due to poor communication security	O2, C2	TC55

Continual Improvement

Following the result of the management review, the MR2 assessed the outcome of the internal audit (IA6) and identified opportunities for improvement noted as

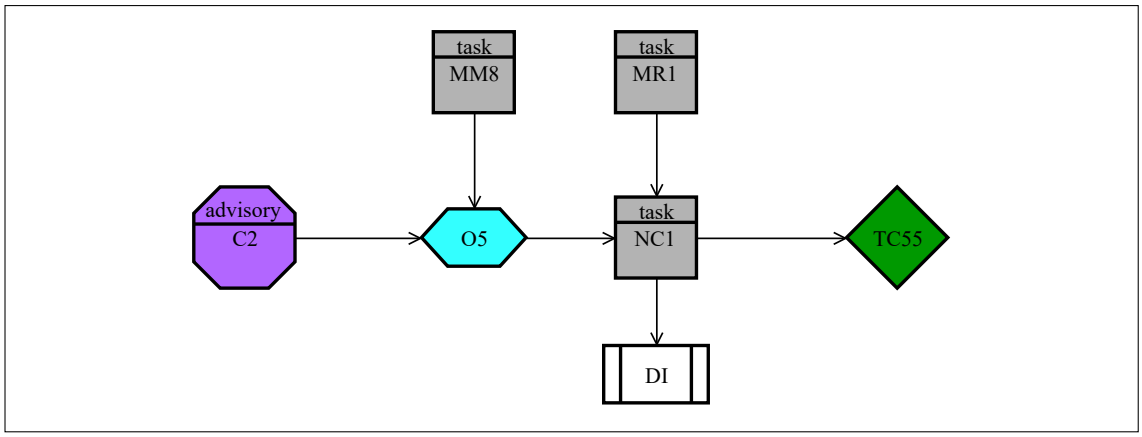


Figure 5.8: Nonconformity and Corrective Action View - AHC

CI1 shown in Figure 5.9.

Table 5.20 describes the continual improvement by indicating an ID number and a brief description of the area of improvement. AHC identified that "secure disposal of media should be extended" (CI1) to include secure disposal of the paper records, hence, recommended an action such as the use of a "shredding service" for the organisation. The result of the progress on CI1 should be recorded and documented according to the procedures in the Documented Information View.

Table 5.20: Register of the action for continual improvement - AHC

ID	Description	Method	Action
CI1	Secure disposal of media should be extended	IA6	Shredding service

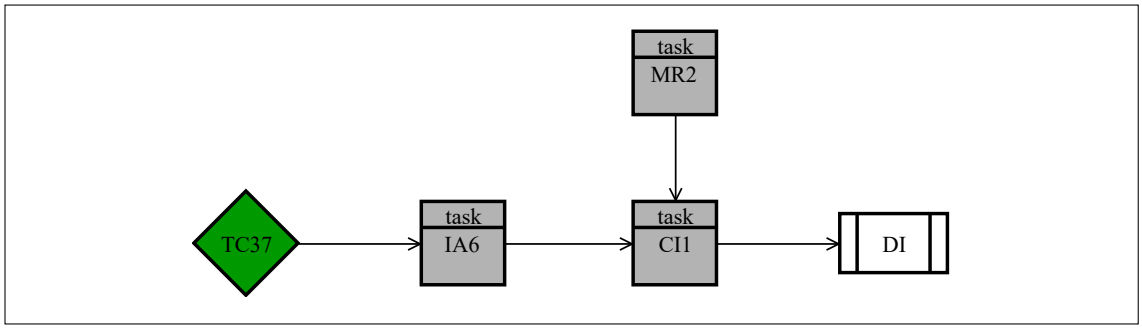


Figure 5.9: Continual Improvement View - AHC

5.4 Evaluation Results

This chapter aims to produce an unbiased and reliable evaluation exercise to the INFORMS framework. Also, the information gathered through the evaluation process should produce outcomes to reflect the overall aim of this exercise. The results of this evaluation reported in two forms, a semi-quantitative analysis of the produced

artefacts using metrics and a qualitative assessment of the features and characteristics of the framework using semi-structured interviews.

A post-implementation analysis used to reassess the conformity status of the organisation with the requirements of the standard upon the implementation of INFORMS. The results of the semi-quantitative analysis provided in the following section. Next, an exit interview of the involved participants pursued to extract empirical conclusions regarding their experience during the use of INFORMS including what they perceive as its contribution and shortcomings.

5.4.1 Metrics Evaluation

The opinion and experiences of the involved participants are potentially subjective and qualitative, hence, the alternative source for evaluating the application of the proposed framework is through the analyses of metrics. This approach provides the semi-quantitative metrics as shown in Table 5.21 able to capture the conceptual and security related completeness of the produced artefacts. Also, it ables to provide further indication of the framework usability and compare them against the baseline described in Table 5.1. The columns in the table incorporate the relevant clause number to the required document or records of the standard, the specific document or record, the readiness level of the organisation prior to the use of the framework, the level of conformity of the organisation in post-implementation of INFORMS and the supporting views or viewpoints in meeting the clauses of the standard.

The results of the post-implementation indicate that almost all mandatory documents and records established after the use of INFORMS, however, the organisation was limited in meeting a small number of documents and records, e.g., Acceptable Use of Assets (Clause A.8.1.3) and Incident Management Procedure (Clause A.16.1.5). While those clauses were not identified through the use of INFORMS, however, the organisation adopted the relevant treatment controls (TC1 and TC113) respectively to meet the requirements of the standard.

Further, the Secure System Engineering Principles (Clause A.14.2.5) was partially satisfied, therefore, provided an opportunity for the continual improvement, and the organisation adopted the treatment control TC144 to fulfil the standard.

Table 5.21: Post-analysis of the AHC's documents and records

Clause	Document/record	Status (pre)	Status (post)	INFORMS View/Control
Part 1: Mandatory				
4.3	Scope of the ISMS	-	++	Scope
5.2	Information security policy	-	++	Policy
6.1.2	Risk assessment and risk treatment methodology	-	++	Technical Viewpoint
6.1.3 d	Statement of Applicability	-	++	Risk Evaluation Risk Treatment
6.1.3 e	Risk treatment plan	-	++	Risk Treatment
6.2	Information security objectives	-	++	Objectives Specification
7.2	Records of training, skills, experience and qualifications	+	++	Actors Description
8.2	Risk assessment report	-	++	Risk Determination
9.1	Monitoring and measurement results	-	++	Monitoring and Measurement
9.2	Internal audit program	+	++	Internal Audit
9.2	Results of internal audits	+	++	Internal Audit
9.3	Results of the management review	+	++	Management review
10.1	Results of corrective actions	+	++	Nonconformity & Corrective Action
A.7.1.2 A.13.2.4	Definition of security roles and responsibilities	-	++	Roles Description
A.8.1.1	Inventory of assets	-	++	Asset Management
A.8.1.3	Acceptable use of assets	-	-	TC1
A.9.1.1	Access control policy	+	++	TC2
A.12.1.1	Operating procedures for IT management	-	++	TC38
A.12.4.1 A.12.4.3	Logs of user activities, exceptions, and security events	-	++	TC23 TC45
A.14.2.5	Secure system engineering principles	-	+	TC144

Continued on next page

Table 5.21: continued from previous page

Clause	Document/record	Status (pre)	Status (post)	INFORMS Viewpoint/View
A.15.1.1	Supplier security policy	-	++	TC58
A.16.1.5	Incident management procedure	-	-	TC113
A.17.1.2	Business continuity procedures	-	++	TC98
A.18.1.1	Statutory, regulatory, and contractual requirements	-	++	Constraints Specification
Part 2: Non-mandatory				
7.5	Procedure for document control	-	++	Documented Information
7.5	Controls for managing records	-	++	Documented Information
9.2	Procedure for internal audit	+	++	Internal Audit
10.1	Procedure for corrective action	+	++	Nonconformity & Corrective Action
A.6.2.1	Bring your own device (BYOD) policy	N/A	N/A	TC82
A.6.2.1	Mobile device and teleworking policy	-	+	TC132
A.8.2.1 A.8.2.2 A.8.2.3	Information classification policy	+	+	Asset Management
A.8.3.2 A.11.2.7	Disposal and destruction policy	-	++	TC37
A.9.2.1 A.9.2.2 A.9.2.4 A.9.3.1 A.9.4.3	Password policy	-	++	TC92 TC154
A.11.1.5	Procedures for working in secure areas	-	+	TC131
A.11.2.9	Clear desk and clear screen policy	-	++	TC22

Continued on next page

Table 5.21: continued from previous page

Clause	Document/record	Status (pre)	Status (post)	INFORMS Viewpoint/View
A.12.1.2 A.14.2.4	Change management policy	-	++	TC145
A.12.3.1	Backup policy	+	++	TC54
A.13.2.1 A.13.2.2 A.13.2.3	Information transfer policy	-	++	TC62
A.17.1.1	Business impact analysis	-	++	Goal Delivery Assessment of Impacts
A.17.1.3	Exercising and testing plan	-	-	TC94

Note:
N/A = Not Applicable - = Not fulfilled
+ = Partially fulfilled ++ = Fulfilled

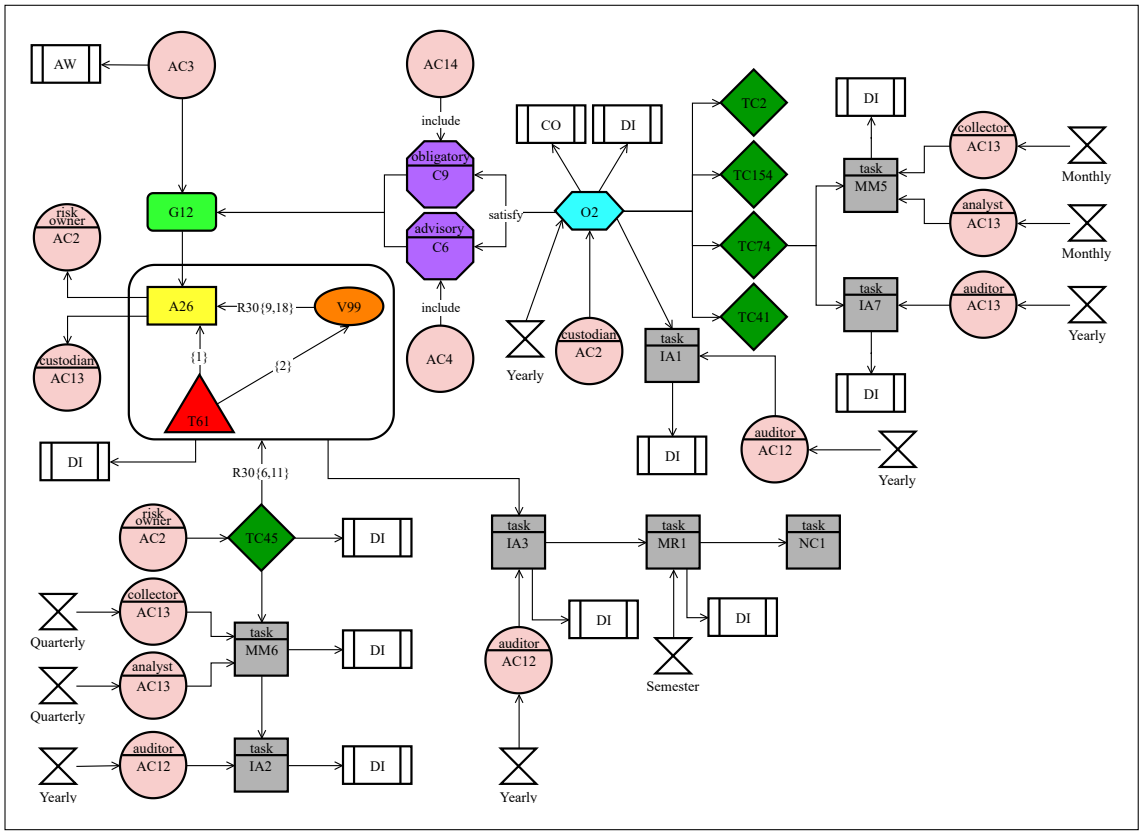


Figure 5.10: Snapshot presentation of all views - AHC

5.4.2 Stakeholders Interview

An extensive set of semi-quantitative metrics measured the applicability of the framework in the previous section; however, some of the insights originated from

the participants were qualitative. Also, the metrics were able to capture the conceptual and security-related completeness of the produced artefacts. On the other hand, they were limited in providing any further indication of their quality.

While the opinions and experiences of the involved participants were potentially subjective, they provided a useful source for the evaluation of the proposed framework. This interview provided an opportunity to receive independent feedback on the usability and effectiveness of INFORMS.

A key outcome gained from the evaluation was that even users with limited knowledge of the standard or the workflow of the ISMS were able to sensibly interact with the framework and create coherent models within a reasonable time-frame. The implementer had no prior knowledge about the requirements of the standard and had no competence in information security or requirements engineering. The implementer was keen to read short and straightforward materials about the standard, however, this was found too abstract and technical.

The implementer indicated that the challenging part was learning about the terms and meaning of the vocabularies used in the standard as well as understanding the relationship structure between the requirements of the standard. This indication is also aligned with the findings of the literature, suggesting that the alternative ad-hoc approaches are limited in what they provide to organisations aiming to implement ISMS.

The participants noted that the simplicity in naming the concepts helped to quickly understand the overall needs of the standard at an abstract level. The Plugin provided to access the graphical notations of the concepts made the modelling efficient, and the implementer could use them without the need for further training of the modelling platform. Despite the large size and information density of some of the created models, the concepts of the modelling language were reasonably clear and easily comprehensible.

The implementer particularly liked the simplicity of the INFORMS meta-model in demonstrating the concepts of the standard, illustrated in one simple diagram. The implementer felt comfortable in exercising most concepts of the INFORMS modelling language including Asset, Threat, Goal, Role and Task. On the other hand, the implementer had to make further enquiry to the researcher to get a better grasp of some concepts such as Constraint, Objective, Vulnerability and Treatment.

The implementer suggested the types of relationships between the concepts became easy once learned all the concepts of the modelling language. He initially expressed concern on following some attributes of the concepts like ID, however, he found it useful once started to use the framework and sketch the models.

When asked about the complexity of the modelling language used by the framework, the implementer noted that the association between the strategic goals and operational level is logically structured by the framework. It promotes businesslike alignment between strategies and operations. It was indicated that the overall application of the process could be demanding in terms of time and complexity, but the available tool support could help to reduce that overhead.

Also, the implementer found the ability to generate prioritisation scenarios as a very positive feature of the framework, as it provided him with flexibility during decision making. Nevertheless, the number of models needed to be instantiated added to its complexity and required some guidance for their successful application.

The implementer suggested that the association between the viewpoints are orderly and easy to follow. Further, the naming of the viewpoints allowed the implementer familiars with some of the viewpoints' titles, e.g., Strategic, Operational, and Technical Viewpoints. The System Viewpoint and Standard Viewpoint became apparent once the researcher explained the reasoning and description of the viewpoints to the participants.

The implementer was able to model the Strategic and Operational Viewpoints following the study of the materials provided to him, which incorporate the right amount of the requirements from the standard.

The implementer had to liaise with the IT contractor to assist with the implementation of the Technical Viewpoint. The implementer found the business-related views of the viewpoint easy to understand, such as the Goal Impact Indicator (GII). The involvement of an expert participant made the implementer confident in identifying and assessing information security risks.

The implementer considered the impact indicators identified by the proposed framework are relevant and it helped the organisation to speculate main consequences that could impact on the operation of the organisation, i.e., impacts on business, financial, legal and privacy.

The security expert who provided expert input in implementing the Technical Viewpoint indicated that some further guidelines or resources for the identification of numerical values for variables related to information security risks (e.g., likelihood, impact) would significantly improve the effectiveness of the risk assessment. Nevertheless, he recognised that the subjectivity involved in the identification of quantitative values for such aspects is an inherent limitation of all risk management frameworks and that the structured and organised approach provided by the framework is a step towards the right direction.

The implementer had a mixed feeling about the Standard Viewpoint since the

nature of the views require inputs from more than one participant including the contribution of a member of IT contractor and a member of the top management. However, it was noted that the participation of multi-users helped to promote the engagement of the top management with establishing, implementing, maintaining and continually improve the ISMS, which is also a requirement of the standard.

5.5 Summary

In this chapter, the INFORMS framework evaluated through a case study to demonstrate how the framework supports the implementation of an ISMS and conforms to the requirements of the standard in an organisation. The framework used by a number of participants from the studied organisation, who provided insight into the organisation's processes and operations. Finally, an exit interview and a post-implementation analysis delivered to evaluate the use and applicability of the framework.

Chapter 6

Conclusion

This chapter presents the overall conclusions by bringing together summaries from the preceding chapters, and by revisiting the aim and objectives of the thesis linked to the outcomes of the research study. Finally, it reflects on the research contribution to knowledge and the opportunities for future research this affords.

6.1 Revisiting the Aim and Objectives

A thorough investigation in how organisations perceive and implement the ISO/IEC 27001 highlighted some critical gaps for those aiming to adopt the standard to the operation of the organisation. The investigation considered what guides are available to support the implementation process of the standard.

This thesis has raised several questions as examined in Section 1.2, sought to investigate and answer these research questions through six objectives.

RO.1 Identify and analyse the relationship between the requirements of the ISO/IEC 27001 Standard.

Our first objective achieved through a methodical study of the ISO/IEC 27000 family of standards as explored in Chapter 2. There are 140 sub-clauses and notes included in clauses 4 to 10 of the standard to incorporate all aspects of the information security management system. While the overall structure of the standard is extensively prescribed in a top to bottom approach, the association between the sub-clauses are intentionally loose to accommodate various methods of implementation suitable to the needs of organisations.

The result of the study identified 22 requirements from the standard. Each requirement had to be explored as an independent concept to build an in-depth knowledge about their significance to the standard. Also, an examination of all concepts as a whole to gather the associations of the standard as one working package. This approach provided great insight and consistency at the interpretation of

the definitions and clauses of the standard. This further developed to establish a consolidated foundation for communicating the terms used in this research.

RO.2 Define a modelling language capable of modelling the requirements of the ISO/IEC 27001 Standard from a security requirements engineering perspective.

In the previous objective, the definitions identified and a list of requirements compiled from the standard. An integral part of the research aimed to bring together concepts from the Goal-oriented Requirements Engineering and the requirements of the standard. The majority of the requirements identified in the standard had no matching correspondence with the existing literature in the GORE. Thus it demanded enhancement of the language and modifications to accommodate the process of the standard. Any proposal for a solution had to consider its applicability and completeness to all requirements of the standard. A total of ten concepts introduced along with ten unique attributes and 11 unique operations between all concepts to meet all clauses of the standard.

Also, a total of ten relationships developed to associate the concepts in the proposed modelling language. An information model demonstrated as meta-model created to underpin the structure of the underlying concepts and relationships. Each concept presented with a unique graphical notation and relationships described with their indicative cardinality.

RO.3 Develop a framework to support the implementation of information security management systems in an organisational setting.

By defining the structure of the modelling language, a conceptual model introduced to enable the modelling and capturing the standard, however, since understanding and managing those requirements require a methodological approach, a structured process known as framework defined to support the implementation of the standard. The information security management system is a complex process that describes the best practice in managing information security, while it has been loosely defined to enhance its applicability to cover any size or nature of the organisation.

The framework introduced 24 views across five viewpoints to cover the overall structure of the ISMS. Each viewpoint designed to capture the various layers of the organisation as well as the corresponding requirements of the standard.

RO.4 Propose a method to address information security risk management per situational needs.

ISO/IEC 27001 is a risk-based standard meaning its approach influence planning and conducting risks to ensure that the processes are focused on matters that are

significant to the organisation for achieving its objectives and strategic aims.

A systematic approach to information security risk management is necessary to establish organisational needs related to information security and to create an effective ISMS. The approach should be suitable for the organisational's environment, and in particular, should be aligned with the overall enterprise risk management.

An information security risk management approach was built as part of the INFORMS framework to address the assessment and evaluation of the risk in information security. It is under the Technical Viewpoint, which represented by seven views to manage risks in an effective and efficient manner where and when they are needed. Information security risk management should be an integral part of all information security activities and to be applied both to the implementation and the ongoing operation of an ISMS.

The risk to assets and goals should be evaluated against the acceptance criteria recognised by the organisation. The risk to information assets could include impacts on the confidentiality, integrity, and availability of the assets while the risk to goals covers broader impacts including business, financial, legal, physical, privacy, social and technical.

RO.5 Develop a process to analyse the effectiveness of information security management systems.

Information security management system is a live process that requires maintenance and continual improvement based on the current and future circumstances of organisations. An effective and fully functional ISMS may take up to 18 months to mature, and it involves more activities than identifying risks and operation of information security.

Continual improvement is a method for identifying opportunities for streamlining the effectiveness of the ISMS. The Standard Viewpoint proposed to meet this objective, including five views to analyse and enhance the effectiveness of the ISMS. This objective reflects at specific parts of the standard which promotes the inspection of the processes in the ISMS as well as identifying non-conformity when arises.

6.2 Main Contributions

The core contribution of this work is an enhancement of the existing literature in security requirements engineering to deliver a framework capable of systematically modelling ISO/IEC 27001 and support the implementation of information security management system. The advancement of this research allows for substantial progress in introducing an approach to meet the limitation of the current gap in the literature.

The following are the contributions of this research to the academic, research community and commercial arena:

RC.1 An iterative framework providing sets of processes to support information security practitioners in implementing an information security management system. The framework supports organisations to conform to the requirements of the ISO/IEC 27001. The processes proposed in the framework enable system implementers and security practitioners to holistically capture, analyse, and implement information security management systems.

The relationships in the framework's processes facilitate a seamless transition between different abstraction of organisational layers via explicit views and procedural rules. This enables an organisation to align between high-level strategic direction and security operational level.

RC.2 A modelling language combining concepts from the security requirements engineering and ISO/IEC 27001 to support the implementation of the information security management system. The language reforms the concepts of security requirements engineering to align with the requirements of the standard.

RC.3 A model-driven architecture with the capacity to manage information security risks in an organisation for the use of information security practitioners. A set of pre-configured processes that guide the assessment of the information security risks in a structured manner. The analysis of the risks enhance the decision-making ability of the organisation's top management and increase the effectiveness of the information security management system.

RC.4 Enhance security requirements engineering in two directions of concept/ language and process in support for the elicitation and exercise of all aspects of information security management systems.

Table 6.1 provides a detailed review of INFORMS against all 22 criteria excerpted from the clauses and sub-clauses of the standard established as part of the systematic review of the literature in Section 2.2.1. The indicative (+) sign in the table denotes the fulfilment of a criterion. It follows an identical method of analysis as shown in Table 2.5, which found two out of 21 relevant studies were able to fulfil the criteria at the Proficient level and the remaining studies were at Basic or Developing stage. However, INFORMS evaluated as Advanced level by fulfilling all the 22 criteria of the standard. The levels of assessment are provided in the note section of the table.

RC.5 Introduce a groundwork for non-security practitioners to understand and analyse the requirements of the standard and cooperate with security practition-

Table 6.1: Satisfying the requirements of the ISO/IEC 27001

Title	Plan														Do			Check			Act		Overall
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	
INFORMS	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	A

Note:
(D) Developing = Fulfil up to 4 criteria out of 22
(B) Basic = Fulfil between 5 to 9 criteria out of 22
(P) Proficient = Fulfil between 10 to 14 criteria out of 22
(A) Advanced = Fulfil more than 15 criteria out of 22

ers in providing inputs to the implementation of information security management systems.

6.3 Future Directions

The development and evaluation of the proposed framework to support the implementation of information security management systems revealed possible directions for future research attempts.

Information Security Best Practices

The process to identify the concepts of the INFORMS modelling language was subjected to two principles. One is being particularly well suited for the needs of the standard, and the other is having broadened definitions to generally being accepted to other information security practices. The latter theory enables the INFORMS modelling language being able to adequately accommodate similar information security best practices such as Cyber Essentials [1] or NIST Cybersecurity Framework.

This makes the research particularly interesting for organisations require to comply with more than one information security practice either to satisfy a client's request or as part of their legal and regulatory obligations.

ISO Standards

Since 2012, the ISO uses a high-level structure for all management systems known as Annex SL. This format helps to streamline the creation of new standards and to eliminate conflicts in management systems. It is a common practice for organisations to implement multi standards related to their services and products in all or part of the organisation. This enables an organisation to benefit from more than one best practice in achieving and integrating high level, common business goals and issues.

The provision of the views in the INFORMS framework developed pragmatically by having a realistic reflection of how ISO standards work and importantly be

[1] UK government-backed scheme provides a set of necessary technical controls to help organisations protect themselves against a range of the most common cyber attacks.

consistent with the requirements of the ISO/IEC 27001. Future work is required to establish the viability of the current views with requirements of other ISO standards. In future investigations, it might be possible to implement more than one standard, e.g., implement and certify to both ISO/IEC 27001 and ISO 9001.

This incorporates similar processes under one holistic approach to eradicate confusions and duplications caused by parallel management systems. However, this may require to propose new views or modify the existing ones. Also, it eliminates potential redundancy at the operational level for organisations deploying multi standards.

Privacy

The announce of regulations like GDPR has increased awareness and legal obligations for organisations on how to process and protect Personally Identifiable Information. Designing and building a privacy-preserving system is challenging since these systems have to address conflicting security properties and system requirements to avoid any security vs privacy trade-off. If security and privacy are addressed together as a unified project, the resulting system will have a security and privacy built-in rather than a bolt-on approach [19].

Even though this work focused on security, the extension of INFORMS to support aspects related to privacy can be explored in future work. A further study could propose a broad approach to introduce views that could accommodate the requirements of the external guidelines or regulations such as GDPR. This supports the analysis of security, privacy, and systems requirements under one integrated framework.

Introduction of ISO/IEC 27701 as the first international privacy standard outlines the requirements for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS). It is an extension to ISO/IEC 27001 for privacy management within the context of the organisation.

Tool support

The current modelling of the concepts uses Draw.io platform, which has limited support for automatic layout and arrangement presentation. While the current features of the platform could support the creation of small-scale models using the INFORMS modelling language, it is not suitable for larger models. A dedicated tool to address the need of the modelling language could improve the usability of the framework. The complexity of the visual models on the decision-making process has not yet been studied within the scope of this work.

Another feature that could enhance the usability of the modelling language is the completeness of the current tool to support the graphical presentation of the

language and its attributes. This has been partly addressed by the introduction of ID in the representation of the concepts rather than describing the labels. It eliminates the visual clutter of complex models, helps the tractability and generating reports. Any new tool is suggested to include the tabulation and other forms of presenting the INFORMS views under one platform; it facilitates the users to complete and implement ISMS in a consistent and coherent approach.

Risk Models

A further study with more focus on devising a method for the automated transformation of security patterns from expert databases such as Common Vulnerabilities and Exposures (CVE)[2] or Common Vulnerability Scoring System (CVSS)[3] to our proposed framework. An investigation is needed to import patterns in the tool support, e.g., replicating a set of security mechanisms to mitigate a specific vulnerability and generating a pattern using the INFORMS concepts in an existing model.

The automated transformation of security controls into security patterns will provide implementers with an expandable library of security patterns, consisting of industry solutions. Also, such a tool could provide implementers with a graphical environment in which they can create goal models using the proposed framework and automatically transform them into other models.

Evaluation

The evaluation of the INFORMS framework applied to a small-sized organisation with a limited number of employees and processes. Although the case study has successfully demonstrated that the framework supports the implementation of the ISMS, it would be interesting to apply the framework to larger organisations or a public sector organisation to compare the results and investigate the experience of the participants.

6.4 Summary

This chapter discussed the overall conclusion and the key contributions of this research according to the aim and objectives of the thesis. It also outlined new avenues to the information security practitioners and organisations to implement information security management systems and move to a closer understanding of the requirements of the standard.

[2]A list of publicly disclosed information security vulnerabilities and exposures to identify and categorise vulnerabilities in software and firmware by creating a standardised identifier for a given vulnerability or exposure.

[3]It provides a method to capture and communicate the characteristics and severity of software vulnerability and produce a numerical score reflecting its impact.

Glossary

accreditation the formal recognition by an independent body, generally known as an accreditation body, that a certification body operates according to international standards. 20

actor an entity that has intentionality and strategic goals within its organisational setting relevant to the scope of the ISMS. 46

asset information system resource. 47

audit systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. 118

availability property of being accessible and usable by an authorized entity. 100

awareness planned programs developed by the organisation for actors doing work under the organisation's control to understand their responsibilities and how their behaviour contributes to the effectiveness and performance of the ISMS. 80

certification the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements. 20

communication process that an organisation conducts to provide, share or obtain information with internal and external actors to increase an actor's involvement with the context of the ISMS. 82

competency ability to apply knowledge and skills to achieve intended results. 87

confidentiality property that information is not made available or disclosed to unauthorized individuals, entities, or processes. 100

constraint stipulation of restrictions and boundaries on assets and goals introduced by an actor. 49

continual improvement ongoing effort to improve performance. 122

custodian individual or entities with approved responsibility by the risk owner to oversight, and have administrative and/or operational responsibility for an asset or group of assets. 90

documented information information required to be controlled and maintained by an organization and the medium on which it is contained. 84

goal actor's strategic interests in the organisation. 50

information security objective organisation-wide information security goals to be achieved. 51

integrity property of accuracy and completeness. 100

likelihood frequency of an incident scenario and an indicator of the severity of an attack. 94

measurement variable to which a value is assigned as the result of measurement. 117

monitoring observe the status of a process. 117

nonconformity non-fulfilment of a requirement. 121

policy proposed strategy by top management for the direction of the organisation's information security. 79

residual risk a potential for reoccurrence of an adverse event after adjusting risk treatment. 110

risk acceptance decision to accept a particular risk through reasoned judgement. 94

risk analysis study the consequence of risk and determine the level of risk. 93

risk evaluation compare the levels of risk with risk criteria to determine whether the significance of risk is acceptable. 93

risk identification recognising and finding the risks and their sources to cause a potential loss. 93

risk owner person or entity with the accountability and authority to manage a risk. 90

risk treatment process to modify risk by encompassing a treatment plan to reduce, retain, avoid, or share the risk. 94

role characteristic of an actor with particular responsibilities to accomplishing the requirements of ISMS. 52

scope precise definition of the physical and abstract boundary of the ISMS implementation. 77

task set of inclusive methods to asses and maintain the performance of ISMS. 54

threat potential cause of an unwanted incident, which may affect information assets or goals. 56

top management person or group of people who directs and controls an organisation at the highest level. 78

treatment treatment is the overall course of action to modify risk. 57

vulnerability weakness of an asset or goal that can be exploited by one or more threats. 58

Bibliography

[1] Travis D. Breaux and Annie I. Anton. Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering*, 34(1):5–20, 2008. Cited on 1

[2] Ed Targett. 6 months, 945 data breaches, 4.5 billion records, 2018. Available at: https://www.cbronline.com/news/global-data-breaches-2018 [Accessed 2019-12-31]. Cited on 1

[3] The Breach Level Index. Data breach database. Available at: https://breachlevelindex.com/data-breach-database [Accessed 2019-12-31]. Cited on 1

[4] Susan Moore. Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017, 2017. Available at: https://www.gartner.com/newsroom/id/3784965 [Accessed 2019-12-31]. Cited on 1

[5] Jane Price Laudon and Kenneth C. Laudon. *Essentials of MIS, global edition.* Pearson Higher Education & Professional Group, 12 edition, 2016. Cited on 1, 12

[6] Kenneth C. Laudon and Jane Price Laudon. *Management information systems: managing the digital firm.* Pearson Higher Education & Professional Group, 10 edition, 2007. Cited on 1

[7] International Organization for Standardization. ISO/IEC 27001 Information security management. Available at: https://www.iso.org/isoiec-27001-information-security.html [Accessed 2019-12-31]. Cited on 2, 20

[8] International Organisation for Standardisation. The ISO survey of management system standard certifications 2017. Technical report, International Organisation for Standardisation, Geneva, Switzerland, 2017. Cited on 2, 21

[9] Daniel Ganji, Haralambos Mouratidis, and Saeed Malekshahi Gheytassi. Towards a Modelling Language for Managing the Requirements of ISO/IEC 27001 Standard. In *5th International Conference on Advances and Trends in Software Engineering (SOFTENG)*, pages 17–23, Valencia, Spain, 2019. IARIA. Cited on 2

[10] ISO 27001 global report. Technical report, IT Governance, 2016. Cited on 2

[11] Gary Hardy. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, 11(1):55–61, 2006. Cited on 3

[12] Luca Compagna, Paul El Khoury, Fabio Massacci, Reshma Thomas, and Nicola Zannone. How to capture, model, and verify the knowledge of legal, security, and privacy experts : a pattern-based approach. In *11th international conference on Artificial intelligence and law*, pages 149–153, Stanford, California, 2007. ACM. Cited on 3

[13] Charles B. Haley, Robin Laney, Jonathan D. Moffett, and Bashar Nuseibeh. Security requirements engineering: a framework for representation and analysis. *IEEE Transactions on Software Engineering*, 34(1):133–153, 2008. Cited on 3, 7

[14] Basie Von Solms. Information Security governance: COBIT or ISO 17799 or both? *Computers and Security*, 24(2):99–104, 2005. Cited on 3

[15] Elizabeth Coles-Kemp. *The anatomy of an information security management system*. PhD thesis, King's College London, University of London, 2008. Cited on 3

[16] Edward W.N. Bernroider and Milen Ivanov. IT project management control and the Control Objectives for IT and related Technology (CobiT) framework. *International Journal of Project Management*, 29(3):325–336, 2011. Cited on 3

[17] Daniel Ganji, Christos Kalloniatis, Haralambos Mouratidis, and Saeed Malekshahi Gheytassi. Approaches to develop and implement ISO/IEC 27001 standard - information security management systems: a systematic literature review. *International Journal On Advances in Software*, 12(3-4):228–238, 2019. Cited on 3

[18] Axel Van Lamsweerde. *Requirements engineering: from system goals to UML models to software specifications*. Wiley, 2009. Cited on 6

[19] Daniel Ganji, Haralambos Mouratidis, Saeed Malekshahi Gheytassi, and Miltos Petridis. Conflicts Between Security and Privacy Measures in Software Requirements Engineering. In Hamid Jahankhani, Alex Carlile, Babak Akhgar, Amie Taal, Ali G. Hessami, and Amin Hosseinian-far, editors, *10th International Conference on Global Security, Safety and Sustainability (ICGS3)*, volume 534, pages 323–334, London, UK, 2015. Springer International Publishing. Cited on 6, 188

[20] Axel Van Lamsweerde and Emmanuel Letier. Handling obstacles in goal-oriented requirements engineering. *IEEE Transactions on Software Engineering*, 26(10):978–1005, 2000. Cited on 6

[21] Juan M. Carrillo de Gea, Joaquin Nicolas, Jose L. Fernandez Aleman, Ambrosio Toval, Christof Ebert, and Aurora Vizcaino. Requirements engineering tools. *IEEE Software*, 28(4):86–91, 2011. Cited on 7

[22] Gilles Goncalves and Aneta Poniszewska Maranda. Role engineering: from design to evolution of security schemes. *Journal of Systems and Software*, 81(8):1306–1326, 2008. Cited on 7

[23] Donald G. Firesmith. Specifying reusable security requirements. *Journal of Object Technology*, 3(1):61–75, 2004. Cited on 7

[24] S. L. Pfleeger and C. P. Pfleeger. Harmonizing privacy with security principles and practices. *IBM Journal of Research and Development*, 53(2):1–12, 2009. Cited on 7

[25] Eric Siu Kwong Yu. Social modeling and i*. In *Conceptual Modeling: Foundations and Applications*, volume 5600, pages 99–121. Springer-Verlag Berlin Heidelberg, 2009. Cited on 7

[26] Eric Siu Kwong Yu. *Modelling strategic relationships for process reengineering*. PhD thesis, University of Toronto, 1995. Cited on 7, 38

[27] Golnaz Elahi and Eric Siu Kwong Yu. A goal oriented approach for modeling and analyzing security trade-Offs. In Christine Parent, Klaus Dieter Schewe, Veda C. Storey, and Bernhard Thalheim, editors, *26th International Conference on Conceptual Modeling*, pages 375–390, Auckland, New Zealand, 2007. Springer, Berlin, Heidelberg. Cited on 7

[28] Lin Liu, Eric Siu Kwong Yu, and John Mylopoulos. Security and privacy requirements analysis within a social setting. In *11th IEEE International Requirements Engineering Conference*, pages 151–161, Monterey Bay, CA, USA, 2003. IEEE. Cited on 7

[29] Daniel Amyot, Sepideh Ghanavati, Jennifer Horkoff, Gunter Mussbacher, Liam Peyton, and Eric Siu Kwong Yu. Evaluating goal models within the goal-oriented requirement language. *International Journal of Intelligent Systems*, 25(8):841–877, 2010. Cited on 7

[30] Eric Siu Kwong Yu. Towards modelling and reasoning support for early-phase requirements engineering. In *3rd IEEE International Symposium on Requirements Engineering*, pages 226–235, Annapolis, MD, USA, 1997. IEEE. Cited on 7

[31] Lawrence Chung, Brian A. Nixon, Eric Siu Kwong Yu, and John Mylopoulos. *Non-functional requirements in software engineering*. Springer US, first edition, 2000. Cited on 8

[32] Paolo Bresciani, Paolo Giorgini, Fausto Giunchiglia, John Mylopoulos, and Anna Perini. Tropos: an agent-oriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3):203–236, 2004. Cited on 8, 38

[33] Angelo Susi, Anna Perini, and John Mylopoulos. The Tropos metamodel and its use. *Informatica*, 29(4):401–408, 2005. Cited on 8

[34] Robert Darimont, E. Delor, Philippe Massonet, and Axel Van Lamsweerde. GRAIL/KAOS: an environment for goal-driven requirements engineering. In *19th International Conference on Software Engineering*, pages 612–613, Boston, Massachusetts, USA, 1997. ACM. Cited on 8

[35] Axel Van Lamsweerde. Engineering requirements for system reliability and security. In *NATO Security through Science Series: Information and Communication Security*, pages 196–238. IOS Press, 2007. Cited on 8

[36] Anne Dardenne, Axel Van Lamsweerde, and Stephen Fickas. Goal-directed requirements acquisition. *Science of Computer Programming*, 20(1-2):3–50, 1993. Cited on 8

[37] Axel Van Lamsweerde, Robert Darimont, and Emmanuel Letier. Managing conflicts in goal-directed requirements engineering. *IEEE Transactions on Software Engineering*, 24(11):908–925, 1998. Cited on 8

[38] Axel Van Lamsweerde. Elaborating security requirements by construction of intentional anti-models. In *26th International Conference on Software Engineering*, pages 148–157. IEEE Computer Society, 2004. Cited on 8

[39] Daniel Mellado, Carlos Blanco, Luis Enrique Sanchez, and Eduardo Fernandez-Medina. A systematic review of security requirements engineering. *Computer Standards & Interfaces*, 32(4):153–165, 2010. Cited on 9

[40] Benjamin Fabian, Seda Gürses, Maritta Heisel, Thomas Santen, and Holger Schmidt. A comparison of security requirements engineering methods. *Requirements Engineering*, 15(1):7–40, 2010. Cited on 9

[41] Fabiano Dalpiaz, Elda Paja, and Paolo Giorgini. Security requirements engineering via commitments. In *1st Workshop on Socio-Technical Aspects in Security and Trust*, pages 1–8, Milan, Italy, 2011. IEEE. Cited on 9

[42] Haralambos Mouratidis and Paolo Giorgini. Secure Tropos: a security-oriented extension of the Tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(02):285–309, 2007. Cited on 9

[43] Haralambos Mouratidis. Secure Tropos: an agent oriented software engineering methodology for the development of health and social care information systems. *International Journal of Computer Science and Security*, 3(3):241–271, 2009. Cited on 9

[44] Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. Addressing privacy requirements in system design: The PriS method. *Requirements Engineering*, 13(3):241–255, 2008. Cited on 9

[45] Haralambos Mouratidis, Shareeful Islam, Christos Kalloniatis, and Stefanos Gritzalis. A framework to support selection of cloud providers based on security and privacy requirements. *Journal of Systems and Software*, 86(9):2276–2293, 2013. Cited on 9, 38

[46] Armstrong Nhlabatsi, Arosha Bandara, Shinpei Hayashi, Charles B. Haley, Jan Jürjens, Haruhiko Kaiya, Atsuto Kubo, Robin Laney, Haralambos Mouratidis, Bashar Nuseibeh, Thein Than Tun, Hironori Washizaki, Nobukazu Yoshioka, and Yijun Yu. Security patterns: comparing modeling approaches. In

Software Engineering for Secure Systems: Industrial and Research Perspectives, pages 75–111. IGI Global, 2010. Cited on 10

[47] William Smart. Lessons learned review of the WannaCry ransomware cyber attack. Technical report, Department of Health and Social Care, 2018. Cited on 10

[48] James Condliffe. A history of Yahoo hacks, 2016. Available at: https://www.technologyreview.com/s/603157/a-history-of-yahoo-hacks/ [Accessed 2019-12-31]. Cited on 10

[49] Ericsson Mobility Report. Technical report, Ericsson, 2019. Cited on 11

[50] EU coordinated risk assessment of the cybersecurity of 5G networks. Technical report, NIS Cooperation Group (EU), 2019. Cited on 11

[51] Effy Oz. *Management information systems*. Cengage Learning, sixth edition, 2008. Cited on 11

[52] Kenneth C. Laudon and Jane Price Laudon. *Essentials of management information systems: managing the digital firm*. Prentice Hall, 6 edition, 2005. Cited on 11, 12

[53] Andrian Wiesmann, Andrew Van Der Stock, Mark Curphey, and Ray Stirbei. A guide to building secure web applications and web services. Technical report, OWASP, 2005. Cited on 12, 13

[54] Mikko Siponen and Robert Willison. Information security management standards: problems and solutions. *Information & Management*, 46(5):267–270, 2009. Cited on 12

[55] David S. Kerr and Uday S. Murthy. The importance of the COBIT framework IT processes for effective internal control over the reliability of financial reporting : an international survey. *Information and management*, 50(1):590–597, 2013. Cited on 13

[56] COBIT 5. Technical report, ISACA, 2012. Cited on 13

[57] Mark Wolden, Raul Valverde, and Malleswara Talla. The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, 48(3):1846–1852, 2015. Cited on 14

[58] Framework for improving critical infrastructure cybersecurity. Technical report, National Institute of Standards and Technology (NIST), 2018. Cited on 14

[59] Cybersecurity Capability Maturity Model (C2M2). Technical Report 1.1, Department of Energy, 2014. Cited on 15

[60] Gamma Secure Systems Limited. History of ISO/IEC 27001. Available at: http://www.gammassl.co.uk/27001/history.php [Accessed 2019-12-31]. Cited on 17

[61] International Organization for Standardization. Certification. Available at: https://www.iso.org/isoiec-27001-information-security.html [Accessed 2019-12-31]. Cited on 20

[62] British Standards Institution. ISO/IEC 27001 information security management. Available at: https://www.bsigroup.com/en-GB/iso-27001-information-security/ [Accessed 2019-12-31]. Cited on 20

[63] Pippa Hemingway and Nic Brereton. What is a systematic review? Technical report, Hayward Medical Communications, 2009. Cited on 21

[64] Barbara A Kitchenham. Guidelines for performing systematic literature reviews in software engineering. Technical report, Keele University, Keele, UK, 2007. Cited on 21

[65] Barbara A Kitchenham. Procedures for performing systematic reviews. Technical report, Keele University, Keele, UK, 2004. Cited on 21

[66] Jane Webster and Richard T Watson. Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly*, 26(2):xiii–xxiii, 2002. Cited on 21

[67] Jessie McGowan, Margaret Sampson, and Carol Lefebvre. An evidence based checklist for the peer review of electronic search strategies (PRESS EBC). *Evidence Based Library and Information Practice*, 5(1):149–154, 2010. Cited on 23

[68] Margaret Rouse. Framework, 2015. Available at: http://whatis.techtarget.com/definition/framework [Accessed 2019-12-31]. Cited on 24

[69] C R Kothari. *Research methodology: methods and techniques*. New Age International Publishers, 2004. Cited on 24

[70] ISO/IEC 27001:2013 Information technology - security techniques - information security management systems - requirements. Technical report, International Organization for Standardization, Geneva, Switzerland, 2013. Cited on 25, 83

[71] British Standard Institution. Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013. Technical report, British Standard Institution, 2014. Cited on 25

[72] Shuchih Ernest Chang and Chienta Bruce Ho. Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3):345–361, 2006. Cited on 26

[73] Shuchih Ernest Chang and Chin-Shien Lin. Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3):438–458, 2007. Cited on 26

[74] Daniel Mellado, Eduardo Fernandez-Medina, and Mario Piattini. A common criteria based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces*, 29:244–253, 2007. Cited on 27

[75] Daniel Mellado, Eduardo Fernandez-Medina, and Mario Piattini. A comparison of the common criteria with proposals of information systems security requirements. In *1st International Conference on Availability, Reliability and Security*, Vienna, Austria, 2006. IEEE. Cited on 27

[76] Muhammad Masood Anwar, Muhammad Faisal Zafar, and Zaheer Ahmed. A proposed preventive information security system. In *2007 International Conference on Electrical Engineering*, pages 1–6, Lahore, Pakistan, 2007. IEEE. Cited on 27

[77] Stefan Fenz, Gernot Goluch, Andreas Ekelhart, and Edgar Weippl. Information security fortification by ontological mapping of the ISO/IEC 27001 standard. In *Pacific Rim International Symposium on Dependable Computing*, pages 381–388, Melbourne, Victoria, Australia, 2007. IEEE Computer Society. Cited on 28

[78] Stefan Fenz. Ontology-based generation of IT-Security metrics. In *ACM Symposium on Applied Computing*, pages 1833–1839, Sierre, Switzerland, 2010. ACM. Cited on 28

[79] Stefan Fenz, Stefanie Plieschnegger, and Heidi Hobel. Mapping information security standard ISO 27002 to an ontological structure. *Information & Computer Security*, 24(5):452–473, 2016. Cited on 28

[80] Daniel Mellado, Eduardo Fernandez-Medina, and Mario Piattini. Security requirements variability for software product lines. In *3rd International Conference on Availability, Reliability and Security*, pages 1413–1420, Barcelona, Spain, 2008. IEEE. Cited on 28

[81] Daniel Mellado, Eduardo Fernandez-Medina, and Mario Piattini. Towards security requirements management for software product lines: a security domain requirements engineering process. *Computer Standards & Interfaces*, 30:361–371, 2008. Cited on 28

[82] Daniel Mellado, Haralambos Mouratidis, and Eduardo Fernandez-Medina. Secure Tropos framework for software product lines requirements engineering. *Computer Standards & Interfaces*, 36(4):711–722, 2014. Cited on 28

[83] Wolfgang Boehmer. Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In *2nd International Conference on Emerging Security Information, Systems and Technologies*, pages 224–231, Cap Esterel, France, 2008. IEEE. Cited on 28

[84] Wolfgang Boehmer. Cost-benefit trade-off analysis of an ISMS based on ISO 27001. In *International Conference on Availability, Reliability and Security*, pages 392–399, Fukuoka, Japan, 2009. IEEE. Cited on 28

[85] Nicolas Mayer, Patrick Heymans, and Raimundas Matulevicius. Design of a modelling language for information system security risk management. In *1st international conference on research challenges in information science*, pages 121–132, Ouarzazate, Morocco, 2007. IEEE. Cited on 28

[86] Nicolas Mayer. *Model-based management of information system security risk*. PhD thesis, University of Namur, 2008. Cited on 28

[87] Nicolas Mayer. A cluster approach to security improvement according to ISO/IEC 27001. In *17th European Systems & Software Process Improvement*

and Innovation, Grenoble, France, 2010. Springer-Verlag Berlin Heidelberg. Cited on 28

[88] Andreas Ekelhart, Stefan Fenz, and Thomas Neubauer. AURUM: a framework for information security risk management. In *42nd Hawaii International Conference on System Sciences*, pages 1–10, Big Island, HI, USA, 2009. IEEE. Cited on 29

[89] Andreas Ekelhart, Stefan Fenz, and Thomas Neubauer. Ontology-based decision support for information security risk management. In *Fourth International Conference on Systems*, pages 80–85, Gosier, Guadeloupe, France, 2009. IEEE. Cited on 29

[90] Thierry Valdevit, Nicolas Mayer, and Béatrix Barafort. Tailoring ISO/IEC 27001 for SMEs: a guide to implement an information security management system in small settings. In *Software Process Improvement: 16th European Conference, EuroSPI*, volume 42, pages 201–212, Alcala (Madrid), Spain, 2009. Springer, Berlin, Heidelberg. Cited on 29

[91] Thierry Valdevit and Nicolas Mayer. A gap analysis tool for smes targeting ISO/IEC 27001 compliance. In *12th International Conference on Enterprise Information Systems*, pages 413–416, Funchal, Madeira - Portugal, 2010. Cited on 29

[92] Veselina Hensel and Kerstin Lemke-Rust. On an integration of an information security management system into an enterprise architecture. In *International Workshop on Database and Expert Systems Applications*, pages 354–358, Bilbao, Spain, 2010. IEEE. Cited on 29

[93] Christian Braun, Felix Wortmann, Martin Hafner, and Robert Winter. Method construction - a core approach to organizational engineering. In *ACM symposium on Applied computing*, pages 1295–1299, Santa Fe, New Mexico, 2005. ACM. Cited on 29

[94] Kurt Schneider, Eric Knauss, Siv Hilde Houmb, Shareeful Islam, and Jan Jurjens. Enhancing security requirements engineering by organisational learning. *Requirements Engineering*, 17(1):35–56, 2012. Cited on 29

[95] Ingo Müller, Jun Han, Jean-Guy Schneider, and Steven Versteeg. Tackling the loss of control: standards-based conjoint management of security requirements for cloud services. In *4th International Conference on Cloud Computing*, pages 573–581, Washington, DC, USA, 2011. IEEE Computer Society. Cited on 30

[96] Ingo Müller, Jun Han, Jean-Guy Schneider, and Steven Versteeg. Idea: a reference platform for systematic information security management tool support. In *Engineering Secure Software and Systems*, pages 256–263, Madrid, Spain, 2011. Springer-Verlag Berlin Heidelberg. Cited on 30

[97] Alan Gillies. Improving the quality of information security management systems with ISO 27000. *The TQM Journal*, 23(4):367–376, 2011. Cited on 30

[98] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. Information security challenge and breaches : novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology*, 2(1):67–75, 2012. Cited on 30

[99] Heru Susanto, Mohammad Nabil Almunawar, and Yong Chee Tuan. A novel method on ISO 27001 reviews: ISMS compliance readiness level measurement. *Computer Science Journal*, 2(1):19–29, 2012. Cited on 30

[100] Heru Susanto, Mohammad Nabil Almunawar, Yong Chee Tuan, and Mehmet Sabih Aksoy. I-Solframework: an integrated solution framework six layers assessment on ultimedia information security architecture policy compliance. *International Journal of Electrical & Computer Sciences*, 12(01):20–28, 2012. Cited on 30

[101] Raydel Montesino, Stefan Fenz, and Walter Baluja. SIEM-based framework for security controls automation. *Information Management & Computer Security*, 20(4):248–263, 2012. Cited on 30

[102] Raydel Montesino and Stefan Fenz. Automation possibilities in information security management. In *European Intelligence and Security Informatics Conference*, pages 259–262, Athens, Greece, 2011. IEEE. Cited on 30

[103] M. P. Azuwa, Rabiah Ahmad, Shahrin Sahib, and Solahuddin Shamsuddin. A propose technical security metrics model for SCADA systems. In *International Conference on Cyber Security, Cyber Warfare and Digital Forensic*, pages 70–75, Kuala Lumpur, Malaysia, 2012. IEEE. Cited on 30

[104] M. P. Azuwa and Rabiah Ahmad. Technical security metrics model in compliance with iso/iec 27001 standard. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 1(4):280–288, 2012. Cited on 30

[105] Kristian Beckers, Stephan Faßbender, Maritta Heisel, and Holger Schmidt. Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation. In *7th International Conference on Availability, Reliability and Security*, pages 242–248, Prague, Czech Republic, 2012. IEEE. Cited on 31

[106] Kristian Beckers, Stephan Faßbender, Maritta Heisel, Jan-Christoph Kuster, and Holger Schmidt. Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches. In *4th International Symposium on Engineering Secure Software and Systems*, pages 14–21, Eindhoven, The Netherlands, 2012. Springer, Berlin, Heidelberg. Cited on 31

[107] Aristeidis Chatzipoulidis, Athanasios Belidis, and Theodoros Kargidis. A risk management approach to information society. *The University of the Fraser Valley Research Review*, 4(3):42–56, 2013. Cited on 31

[108] Abbass Asosheh, Parvaneh Hajinazari, and Hourieh Khodkari. A practical implementation of ISMS. In *7th International Conference on e-Commerce in Developing Countries with focus on e-Security*, volume 11, Kish Island, Iran, 2013. IEEE. Cited on 31

[109] Kristian Beckers, Isabelle Cote, Stephan Faßbender, Maritta Heisel, and Stefan Hofbauer. A pattern-based method for establishing a cloud-specific information security management system. *Requirements Engineering*, 18(4):343–395, 2013. Cited on 31

[110] Kristian Beckers, Maritta Heisel, Isabelle Côté, Ludger Goeke, and Selim Güler. Structured pattern-based security requirements elicitation for clouds. In *International Conference on Availability, Reliability and Security*, pages 465–474, Regensburg, Germany, 2013. IEEE. Cited on 31

[111] Kristian Beckers, Stephan Faßbender, and Maritta Heisel. A meta-model approach to the fundamentals for a pattern language for context elicitation. In *18th European Conference on Pattern Languages of Program*, page 28, Irsee, Germany, 2013. ACM. Cited on 31

[112] Kristian Beckers, Holger Schmidt, Jan-Christoph Kuster, and Stephan Faßbender. Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In *6th International*

Conference on Availability, Reliability and Security, pages 327–333, Vienna, Austria, 2011. IEEE Computer Society. Cited on 31

[113] Kristian Beckers, Maritta Heisel, Bjornar Solhaug, and Ketil Stolen. *ISMS-CORAS : A structured method for establishing an ISO 27001 compliant information security management system*. Springer, Cham, 2014. Cited on 31

[114] Kristian Beckers. *Supporting ISO 27001 establishment with CORAS*. Springer, Cham, 2015. Cited on 31

[115] Haralambos Mouratidis. Secure software systems engineering: The secure Tropos approach. *Journal of Software*, 6(3):331–339, 2011. Cited on 38, 61

[116] Peter Carey. *Data Protection: A Practical Guide to UK and EU Law*. Oxford University Press, fifth edition, 2018. Cited on 49

[117] Haralambos Mouratidis. *A security oriented approach in the development of multiagent systems: applied to the management of the health and social care needs of older people in England*. PhD thesis, University of Sheffield, 2004. Cited on 61

[118] Object Management Group. Unified Modeling Language. Technical report, Obeject Management Group (OMG), 2011. Cited on 75

[119] Martin Fowler. *UML distilled: a brief guide to the standard object modeling language*. Addison-Wesley Professional, thrid edition, 2003. Cited on 75

[120] ISO/IEC 27000:2014 Information technology - security techniques - information security management systems - overview and vocabulary. Technical report, International Organization for Standardization, Geneva, Switzerland, 2014. Cited on 78, 95

[121] Bill Gardner and Valerie Thomas. *Building an information security awareness program: defending against social engineering and technical threats*. Syngress, 2014. Cited on 81

[122] Heru Susanto and Mohammad Nabil Almunawar. Information security awareness: a marketing tools for corporate's business processes. *Computer Science Journal*, pages 1–12, 2012. Cited on 81

[123] ISO/IEC 27003:2017 Information technology - security techniques - information security management systems - guidance. Technical report, International Organization for Standardization, Geneva, Switzerland, 2017. Cited on 81

[124] ISO/IEC 27003:2010 Information technology - security techniques - information security management system implementation guidance. Technical report, International Organization for Standardization, Geneva, Switzerland, 2010. Cited on 85, 110

[125] ISO/IEC 27005:2011 Information technology - security techniques - information security risk management. Technical report, International Organization for Standardization, Geneva, Switzerland, 2011. Cited on 93, 107, 109, 110

[126] Special publication 800-30, guide for conducting risk assessments. Technical report, National Institute of Standards and Technology (NIST), 2012. Cited on 95

[127] ClearSwift. The enemy within research, 2013. Available at: https://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [Accessed 2019-12-31]. Cited on 96

[128] David Hutter. Physical security and why it is important. Technical report, SANS Institute, 2016. Cited on 102

[129] Thomas R. Peltier. *Information Security Risk Analysis*. Auerbach Publications, 2nd edition, 2005. Cited on 110

[130] G.T. Doran. There's a S.M.A.R.T. way to write management's goals and objectives. *Management Review*, 70(11):35–36, 1981. Cited on 115

[131] Carolyn B. Seaman. Qualitative methods in empirical studies of software engineering. *IEEE Transactions on Software Engineering*, 25(4):557–572, 1999. Cited on 125

[132] Barbara Kitchenham, Stephen Linkman, and David Law. DESMET: A methodology for evaluating software engineering methods and tools. *Computing and Control Engineering Journal*, 8(3):120–126, 1997. Cited on 125

[133] Shari Lawrence Pfleeger. Design and Analysis in Software Engineering. *Acm Sigsoft*, 19(4):16–20, 1994. Cited on 125

[134] Izak Benbasat, David K. Goldstein, and Melissa Mead. The case research strategy in studies of information systems. *MIS Quarterly: Management Information Systems*, 11(3):369–386, 1987. Cited on 125

[135] Arlene Fink. *The Survey Handbook*. The Survey Handbook. SAGE Publications, 1995. Cited on 126

[136] Per Runeson, Martin Host, Austen Rainer, and Bjorn Regnell. *Case study research in software engineering: guidelines and examples.* John Wiley & Sons, Inc., 2012. Cited on 126

[137] Robert K. Yin. *Case Study Research: Design and Methods.* Applied Social Research Methods. SAGE Publications, 2009. Cited on 128

[138] Timothy C. Lethbridge, Susan Elliott Sim, and Janice Singer. Studying software engineers: Data collection techniques for software field studies. *Empirical Software Engineering*, 10(3):311–341, 2005. Cited on 129

Appendix A

Threat Catalogue

Table A.1: Threat catalogue

ID	Threat
T1	Abuse of rights
T2	Access to the network by unauthorized persons
T3	Bankruptcy of key supplier
T4	Bomb threat
T5	Breach of contractual relations
T6	Breach of legislation
T7	Business disaster
T8	Casual oversight
T9	Communication infiltration
T10	Compromising confidential information
T11	Concealing user identity
T12	Corruption of data
T13	Damage caused by a third party
T14	Damage to communication lines/cables
T15	Damages resulting from penetration testing
T16	Data breach
T17	Data from untrustworthy sources
T18	Defacement
T19	Destruction of equipment or media
T20	Destruction of records
T21	Deterioration of storage media
T22	Disaster (human caused)
T23	Disaster (natural)
T24	Disclosure of information
T25	Disclosure of passwords
T26	Dust, corrosion, freezing

Continued on next page

Table A.1: continued from previous page

ID	Threat
T27	Earthquake
T28	Eavesdropping
T29	Embezzlement
T30	Environmental contamination
T31	Equipment failure
T32	Equipment malfunction
T33	Errors in maintenance
T34	Extremes of temperature and humidity
T35	Failure of air-conditioning
T36	Failure of network components
T37	Failure of power supply
T38	Failure of telecommunication equipment
T39	Failure of water supply
T40	Failure of website
T41	Falsification of records
T42	Fire
T43	Flood
T44	Forging of rights
T45	Fraud
T46	Hacking
T47	Hardware failure
T48	Hurricane
T49	Illegal import/export of software
T50	Illegal processing of data
T51	Illegal use of software
T52	Industrial espionage/spying
T53	Industrial strike
T54	Information leakage
T55	Insufficient or untested backups
T56	Interruption of business processes
T57	Lightning
T58	Loss of key personnel
T59	Loss of power supply
T60	Loss of support services
T61	Loss of system integrity
T62	Maintenance error
T63	Major accident
T64	Malicious code
T65	Malicious software (e.g. viruses)

Continued on next page

Table A.1: continued from previous page

ID	Threat
T66	Masquerading of user identity
T67	Misrouting or rerouting of messages
T68	Misuse of audit tools
T69	Misuse of information systems
T70	Misuse of resources
T71	Operational support staff error
T72	Pollution
T73	Power fluctuation
T74	Recovery of information from disposed media
T75	Remote spying
T76	Repudiation
T77	Sabotage (Wilful damage)
T78	Social engineering
T79	Software failure
T80	Software malfunction
T81	Staff shortage
T82	Tampering with hardware
T83	Tampering with software
T84	Terrorist attacks
T85	Theft/loss of equipment
T86	Theft/loss of media or documents
T87	Thunderstroke
T88	Traffic overloading
T89	Transmission errors
T90	Unauthorised use of storage media
T91	Unauthorized access to the IS
T92	Unauthorized changes of records
T93	Unauthorized installation of software
T94	Unauthorized physical access
T95	Unauthorized use of copyright material
T96	Unauthorized use of software
T97	Unintentional change of data in an IS
T98	Use of network facilities in an unauthorised way
T99	User error (accidental)
T100	Vandalism
T101	Water damage

Appendix B

Vulnerability Catalogue

Table B.1: Vulnerability catalogue

ID	Vulnerability
V1	Absence of personnel
V2	Complicated user interface
V3	Critical System vulnerabilities due to insufficient patch management
V4	Default passwords not changed
V5	Disposal of storage media without deleting data
V6	Excessive privileges due to lack of a user access review
V7	Failure to adhere to company policies
V8	Inadequate back-up testing
V9	Inadequate cabling security
V10	Inadequate capacity management
V11	Inadequate change management
V12	Inadequate classification/labelling of information
V13	Inadequate control of physical access
V14	Inadequate control over system access
V15	Inadequate incident reporting arrangements
V16	Inadequate internal/external audit
V17	Inadequate maintenance
V18	Inadequate network management
V19	Inadequate or irregular backup
V20	Inadequate physical protection
V21	Inadequate protection of cryptographic keys
V22	Inadequate recruitment procedures
V23	Inadequate replacement of older equipment
V24	Inadequate security awareness
V25	Inadequate security training of employees
V26	Inadequate segregation of duties

Continued on next page

Table B.1: continued from previous page

ID	Threat
V27	Inadequate segregation of operational and testing facilities
V28	Inadequate supervision of employees
V29	Inadequate supervision of vendors
V30	Incomplete specification for software development
V31	Incorrect date
V32	Incorrect parameter set up
V33	Insufficient authentication mechanism and controls
V34	Insufficient change control process leading to unauthorized changes
V35	Insufficient contingency planning
V36	Insufficient enforcement of secure deletion and disposal process
V37	Insufficient incident response plan
V38	Insufficient maintenance
V39	Insufficient media encryption
V40	Insufficient or irregular water supply
V41	Insufficient physical controls protecting equipment
V42	Insufficient software testing
V43	Lack of access control policy
V44	Lack of anti-virus and Malware Prevention
V45	Lack of audit trail
V46	Lack of care at disposal
V47	Lack of clean desk and clear screen policy
V48	Lack of control over the input and output data
V49	Lack of documentation
V50	Lack of effective change control
V51	Lack of environmental monitoring
V52	Lack of failover mechanisms for the system
V53	Lack of identification and authentication mechanisms
V54	Lack of logging and monitoring controls
V55	Lack of mechanism to prevent data loss
V56	Lack of monitoring mechanisms
V57	Lack of network security controls
V58	Lack of or poor implementation of internal audit
V59	Lack of periodic equipment replacement schemes
V60	Lack of physical protection of the building, doors and windows
V61	Lack of policies for the correct use of telecommunications media & messaging
V62	Lack of policy for the use of cryptography
V63	Lack of procedure for removing access rights upon termination of employment
V64	Lack of proof of sending or receiving messages
V65	Lack of protection for mobile equipment

Continued on next page

Table B.1: continued from previous page

ID	Threat
V66	Lack of redundancy
V67	Lack of redundant network infrastructure
V68	Lack of redundant power supply
V69	Lack of transmission encryption leading to interception of unencrypted data
V70	Lack of user monitoring and periodic access review
V71	Lack of validation of the processed data
V72	Location vulnerable to flooding
V73	No 'logout' when leaving the work station
V74	Poor joint cabling
V75	Poor password management
V76	Poor selection of test data
V77	Possible security misconfiguration in system due to lack of security and hardening reviews
V78	Possible weak Passwords due to lack of password complexity controls
V79	Single copy
V80	Single point of failure
V81	Susceptibility to humidity, dust, soiling
V82	Susceptibility to temperature
V83	Susceptibility to voltage variations
V84	Too much power in one person
V85	Transfer of passwords in clear
V86	Unauthorized access to the system due to lack of a formal user provisioning process
V87	Uncontrolled copying of data
V88	Uncontrolled download from the Internet
V89	Uncontrolled use of information systems
V90	Undocumented software
V91	Unmotivated employees
V92	Unprotected communication link
V93	Unprotected password tables
V94	Unprotected public network connections
V95	Unprotected sensitive traffic
V96	Unprotected storage
V97	Unstable power grid
V98	Unsupervised work by outside contractors
V99	Untraceable user actions due to generic accounts
V100	User rights are not reviewed regularly
V101	Well known flaws in the software
V102	Wrong allocation of access rights

Appendix C

Statement of Applicability

Table C.1: Statement of Applicability for the AHC Limited

Annex A	**Adopted Y/N**	**Control Agent**	**Annex A**	**Adopted Y/N**	**Control Agent**
A.5.1.1	N	-	A.8.3.2	Y	R6 - TC37 R27 - TC37
A.5.1.2	N	-	A.8.3.3	N	-
A.6.1.1	N	-	A.9.1.1	Y	R5 - TC2 R18 - TC2
A.6.1.2	N	-	A.9.1.2	N	-
A.6.1.3	N	-	A.9.2.1	N	-
A.6.1.4	N	-	A.9.2.2	N	-
A.6.1.5	N	-	A.9.2.3	N	-
A.6.2.1	N	-	A.9.2.4	N	-
A.6.2.2	N	-	A.9.2.5	N	-
A.7.1.1	N	-	A.9.2.6	N	-
A.7.1.2	N	-	A.9.3.1	Y	R10 - TC154
A.7.2.1	N	-	A.9.4.1	N	-
A.7.2.2	Y	R12 - TC135	A.9.4.2	N	-
A.7.2.3	N	-	A.9.4.3	Y	R23 - TC92
A.7.3.1	N	-	A.9.4.4	N	-
A.8.1.1	N	-	A.9.4.5	N	-
A.8.1.2	N	-	A.10.1.1	N	-
A.8.1.3	N	-	A.10.1.2	N	-
A.8.1.4	N	-	A.11.1.1	N	-
A.8.2.1	N	-	A.11.1.2	Y	R2 - TC95
A.8.2.2	N	-	A.11.1.3	Y	R1 - TC131
A.8.2.3	N	-	A.11.1.4	N	-
A.8.3.1	N	-	A.11.1.5	N	-

Continued on next page

Table C.1: continued from previous page

Annex A	Adopted Y/N	Control Agent	Annex A	Adopted Y/N	Control Agent
A.11.1.6	N	-	A.14.2.1	N	-
A.11.2.1	N	-	A.14.2.2	Y	R17 - TC145
A.11.2.2	Y	R21 - TC143	A.14.2.3	N	-
A.11.2.3	N	-	A.14.2.4	N	-
A.11.2.4	N	-	A.14.2.5	N	-
A.11.2.5	N	-	A.14.2.6	N	-
A.11.2.6	N	-	A.14.2.7	N	-
A.11.2.7	N	-	A.14.2.8	N	-
A.11.2.8	N	-	A.14.2.9	N	-
A.11.2.9	Y	R13 - TC22	A.14.3.1	N	-
A.12.1.1	Y	R15 - TC38 R26 - TC38 R29 - TC38	A.15.1.1	Y	R7 - TC58
A.12.1.2	N	-	A.15.1.2	N	-
A.12.1.3	Y	R11 - TC18	A.15.1.3	N	-
A.12.1.4	N	-	A.15.2.1	Y	R8 - TC74
A.12.2.1	N	-	A.15.2.2	N	-
A.12.3.1	N	-	A.16.1.1	N	-
A.12.4.1	Y	R16 - TC45 R30 - TC45	A.16.1.2	N	-
A.12.4.2	N	-	A.16.1.3	N	-
A.12.4.3	N	-	A.16.1.4	N	-
A.12.4.4	N	-	A.16.1.5	N	-
A.12.5.1	N	-	A.16.1.6	N	-
A.12.6.1	N	-	A.16.1.7	N	-
A.12.6.2	N	-	A.17.1.1	Y	R3 - TC50
A.12.7.1	N	-	A.17.1.2	Y	R20 - TC98
A.13.1.1	Y	R14 - TC86	A.17.1.3	N	-
A.13.1.2	Y	R28 - TC14	A.17.2.1	N	-
A.13.1.3	N	-	A.18.1.1	N	-
A.13.2.1	Y	R4 - TC62 R19 - TC62	A.18.1.2	N	-
A.13.2.2	N	-	A.18.1.3	N	-
A.13.2.3	N	-	A.18.1.4	N	-
A.13.2.4	N	-	A.18.1.5	N	-
A.14.1.1	N	-	A.18.2.1	N	-
A.14.1.2	N	-	A.18.2.2	N	-
A.14.1.3	Y	R24 - TC104	A.18.2.3	N	-

Appendix D

Publication

Parts of the research presented in the thesis has been peer-reviewed and published in below conferences. Further publications are currently under review in relevant journal and conference.

1. D. Ganji, H. Mouratidis, S. Malekshahi Gheytassi, and M. Petridis. Conflicts Between Security and Privacy Measures in Software Requirements Engineering. In H. Jahankhani, A. Carlile, B. Akhgar, A. Taal, A. G. Hessami, and A. Hosseinian-far, editors, 10th International Conference on Global Security, Safety and Sustainability (ICGS3), volume 534, pages 323-334, London, UK, 2015. Springer International Publishing.
2. D. Ganji, H. Mouratidis, and S. Malekshahi Gheytassi. Towards a Modelling Language for Managing the Requirements of ISO/IEC 27001 Standard. In 5th International Conference on Advances and Trends in Software Engineering (SOFTENG), pages 17-23, Valencia, Spain, 2019. IARIA.
3. D. Ganji, C. Kalloniatis, H. Mouratidis, and S. Malekshahi Gheytassi. Approaches to develop and implement ISO/IEC 27001 standard - information security management systems: a systematic literature review. International Journal On Advances in Software, 12(3-4):228-238, 2019.