Managing Security and Compliance Risks of Outsourced IT Projects

Moneef Almutairi

School of Computing

Newcastle University

In Partial Fulfilment of the Requirements for the Degree of

Doctor of Philosophy

April 2019

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this thesis are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This thesis is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements.

Dedication

I would like to dedicate this thesis to my wife, sons, family, and my country.

Acknowledgements

My deepest thanks must go firstly to my first supervisor, Dr Steve Riddle. Throughout my PhD journey he has spared me his valuable time to discuss the various aspects of this research. His input helped me to formulate the research objectives, and kept me focused on the research challenges. He has given me invaluable encouragement and feedback on this thesis. My second supervisor, Dr Paul Ezhilchelvan, also generously gave his support and guidance, and I thank him for the time he took to help me. Both of these collaborations provided me with meaningful insights into the various phases of research, including technical writing and publications. Most importantly, I would like to thank my wife and sons for unselfishly allowing me the space and time to complete this project – I could not have done it without their support.

Abstract

Several sources of constraints, such as business, financial and legal, can lead organisations to outsource some of their IT services. As a consequence, different security risks may be introduced, such as confidentiality, integrity and availability risks. Analysing and managing the potential security risks in the early stages of project execution allow organisations to avoid or mitigate the impact of these security risks. Several organisations have adopted ISMS standards and frameworks in an endeavour to manage outsourced IT project security risks. In this thesis, existing ISMS standards and frameworks have been reviewed and analysed to assess their ability to effectively manage the security and compliance risks of outsourced IT projects and satisfy their security needs. The review reveals that existing ISMS standards and frameworks represent only general security recommendations and do not consider variation in security requirements from one organisation to another. There is also a lack of adequate guidance for implementing or complying with these standards and frameworks, and they are not designed to manage the security and compliance risks of outsourced IT projects. To overcome these weaknesses, a new framework has been introduced. The framework is a structured approach that is designed to manage variation in security requirements, as well as provide a methodology to guide organisations for the purpose of security management and implementation. The framework was evaluated using different evaluation methods including a focus group, questionnaire, and case study, which were also used to generate recommendations and suggestions for improvements. The evaluation results confirmed that the framework provided the participants with an effective approach for managing security and compliance risks in the outsourcing context. It was understandable, easy to use, and independent from different constraints such as project size, cost or execution time. The framework is now ready to be put into practice by organisations that intend to outsource their IT services partially or totally.

Table of Contents

List of Tables

List of Figures

Glossary

IT	Information Technology
IS	Information System
RFP	Request For Proposal
NDA	Non-Disclosure Agreement
SLA	Service Level Agreement
ISMS	Information Security Management System
ISO/IEC	International Standards Organization (ISO) and the International Electro-technical Commission (IEC)
NIST	National Institute of Standards and Technology
COBIT	Control Objectives for Information and related Technology
ISACA	Information Systems Audit and Control Association
ITIL	Information Technology and Infrastructure Library
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
IST	Information Society Technologies
UML	Unified Modelling Language
CCTA	Central Computer and Telecommunications Agency
CRAMM	CCTA Risk Analysis and Management Method
SABSA	Sherwood Applied Business Security Architecture
SSE-CMM	Systems Security Engineering - Capability Maturity Model
PMBOK	Project Management Body of Knowledge
PRINCE2	Projects In Controlled Environments
ICB	International Competence Baseline

PMI	Project Management Institute
IPMA	International Project Management Association
OGC	Office of Government Commerce
RAM	Responsibility Assignment Matrix
RACI	Responsible, Accountable, Consult, and Inform
API	Advanced Passenger Information
PNR	Passenger Name Record
RCS	Reservation Control System
DCS	Departure Control System

Chapter 1 Introduction

1.1 Introduction

In recent years, outsourcing has gained more popularity among different organisations in both the public and private domains. The Information Technology (IT) outsourcing market was estimated at $288 billion in 2013 with a 5.9% compound annual growth rate until 2018 [1]. The appearance of new forms of outsourcing arrangements, such as business benefits contracting and co-operative outsourcing, in addition to the spread of cloud computing, has increased the shift towards outsourcing [2]. Software development, systems maintenance, storage operations, and hardware and data management [3], which used to be the responsibility of the IT department of any organisation, are examples of modern outsourcing business practices.

The rapid technological changes and heightened competition have forced some organisations to refocus their IT work on core and strategic business activities and to outsource their routine and non-strategic IT activities to third parties, who can deliver such services in a better and more efficient way [3]. Thus, the time and effort spent by organisations on building and maintaining their internal IT infrastructure are reduced; instead they concentrate their effort and resources on how to use information effectively and efficiently, and on how to build analytical tools that can provide better IT business management [3].

The term *outsourcing* is not only used in the IT field; it can be used to reflect any business practice that involves contracting with external providers for delivering specific services. This business practice can be used in any business type, and can be used for services such as IT, human resources and help desk functions. The growth of IT outsourcing has been influenced by many factors, one of which is the increased acceptance by organisations of the Internet as a major means of communication. The other important factor is the cost reductions that outsourcing can provide to organisations [4, 5].

Outsourcing is an attractive option for organisations, offering benefits including cost reduction, quality improvement, and the opportunity to concentrate on core business activities [6-8]. However, it is an option that must be managed properly as it brings risks, such as security and contract violations, and the loss of technology skills for the organisation [7, 9, 10]. Failure to manage these risks could lead to major issues not only in a particular project, but also for the entire organisation or business [11].

As the growth of outsourcing rapidly increases, information systems become more complex and comprise different entities. Due to the complexity of information systems and the need to integrate new IT services with the existing IT services of organisations, security and compliance risks arise as major challenges for different organisations that intend to outsource their IT services. Confidentiality breaches, auditing compliance, heterogeneity management of IT services, continuity management and lack of security awareness are examples of challenges that can affect organisations if they are not properly addressed. The insufficiency of existing solutions for managing security and compliance risks exposes these organisations to different security and compliance risks, such as the trust that providers apply proper security controls, the ability or willingness of providers to comply with the security policies of the organisation and the trust that the provider will not abuse an organisation's proprietary information or knowledge[2, 12].

While many organisations have adopted Information Security Management System (ISMS) standards and frameworks to secure their information systems, the outsourcing context is still not covered adequately by these standards and frameworks. Even for conventional contexts, these standards and frameworks only represent general security recommendations and do not take into account how security requirements differ from one organisation to another [13]. Moreover, there is no adequate guidance for implementing or complying with such standards and frameworks, nor are they designed to manage the security and compliance risks of outsourced IT projects [14]. Updating these standards

and frameworks to fit the outsourced IT project context makes them more complicated, and increases time and resource consumption. Therefore, this research studies how to effectively manage the security and compliance risks of outsourced IT projects that need to be integrated with clients' information systems.

1.2 Research Motivation

Outsourcing benefits have attracted many organisations and have dominated their decision about whether or not to outsource some functions of their information systems. Other considerations such as security and compliance risks have not been given much attention [15].

The lack of a comprehensive methodology that is capable of effectively managing the security and compliance risks of outsourced IT projects was the major motivation for conducting this research.

To minimise the security and compliance risks of outsourced IT projects, we propose several recommendations that aim to improve the overall security management of organisations. The security programme or framework should comprise different features such as aligning security management with project management, establishing a comprehensive methodology for managing security requirements, managing security risks from different perspectives, managing compliance, and improving flexibility and usability.

As a response to this motivation, we have developed a framework, called the OSCR framework (Outsourcing Security and Compliance Risks framework), that takes into account the recommendations for improving the overall security management of the organisation when outsourcing. The framework is also designed to benefit from the strengths of existing ISMS standards and frameworks and to avoid their weaknesses, as it will be explained in detail in this research.

1.3 Research Questions

In this research, our main question focuses on managing the security and compliance risks of outsourced IT projects effectively. To help answer this question, two sub-questions were asked and answered in this research. The main research question and sub-questions are as follows:

1- *How can we manage the security and compliance risks of outsourced IT projects effectively?*
   a. *What are the strengths and weaknesses of existing security standards and frameworks for managing the security and compliance risks of outsourced IT projects?*
   b. *What are the requirements for managing the security and compliance risks of outsourced IT projects?*

1.4 Research Objectives

This research aims to develop a framework capable of effectively managing the security and compliance risks of outsourced IT projects. The research objectives encompass the following:

- Analysing outsourcing business practices and identifying their benefits and risks, and all other processes and arrangements associated with them, as well as identifying security needs for the outsourcing context.
- Reviewing existing ISMS standards and frameworks in order to assess their ability to manage security and compliance risks in the outsourcing context and to identify their focus, strengths, and weaknesses.
- Developing a comprehensive methodology (framework) capable of effectively managing the security and compliance risks of outsourced IT projects.

- Evaluating the proposed comprehensive methodology (framework) using diverse empirical evaluation methods to assess the applicability of the framework for the outsourced IT project context.

1.5 Research Methodology

To answer the research questions and achieve the research objectives, a research methodology was developed and put into practice. The following highlights the research methodology that has been followed in this research:

- **Literature review:** this first step of the research methodology aims to analyse outsourcing business practices in order to identify their benefits and risks, and all other processes and arrangements associated with them, as well as identifying security issues with outsourcing business practices. Based on this review, the security needs of the outsourcing context can be identified.
- **Related work review:** the research methodology, as a second step, concentrates on reviewing existing ISMS standards and frameworks. The aim of this review is to assess their ability to meet outsourcing security needs and to identify their strengths and weaknesses for managing the security and compliance risks of outsourced IT projects.
- **Requirements identification:** the research methodology in its third step identifies requirements for effectively managing the security and compliance risks of outsourced IT projects. The requirements identification will be drawn based on the outcomes of the review of the literature and existing ISMS standards and frameworks.
- **Framework development:** as a fourth step in the research methodology, we will develop a framework (the OSCR framework) that is expected to effectively manage the security and compliance risks of outsourced IT projects. The framework should meet the identified requirements as well as overcome the weaknesses of the existing ISMS standards and frameworks.

- **Framework evaluation:** the final step of our methodology will be to evaluate the framework. Different empirical evaluation methods will be used (e.g. case study, focus group). The aims of this evaluation include assessing the ability of the framework to effectively manage the security and compliance risks of outsourced IT projects as well as assessing its applicability for the outsourcing context.

1.6 Research Contributions

The major contribution of this research is the framework. Other contributions comprise the analysis of outsourcing, the related work review, and research publications. The following briefly describes these contributions:

- **The OSCR framework:** this is designed to manage the security and compliance risks of outsourced IT projects effectively. The OSCR framework is expected to contribute to the body of knowledge as follows:
    1) Providing a comprehensive methodology for managing the security and compliance risks of outsourced IT projects.
    2) Introducing the concept of aligning security management with project management in the outsourcing context.
    3) Designing a threat classification approach for the outsourcing context.
    4) Enhancing security compliance throughout project execution.
    5) Improving security risk assessment by providing qualitative and semi-quantitative ranges of the probability and magnitude of security threats in the outsourcing context.
    6) Achieving promising features such as flexibility, simplicity and continuous improvement.
- **Outsourcing analysis:** this analyses outsourcing business practices including their benefits, processes, and risks. As a result of this analysis, outsourcing security needs will be identified.

- **Related work review:** this provides an assessment of the existing ISMS standards and frameworks related to security and compliance risk management in the outsourcing context. Their focus, strengths and weaknesses will be identified.
- **Research publications:** six publications have been produced as a result of this research. Section 1.7 provides more details of these publications.

1.7 Research Publications

During the research stages, six publications have been produced. The following describes these publications in more detail:

- M. Almutairi and S. Riddle, "State of the art of IT outsourcing and future needs for managing its security risks," *in (IEEE) 2018 International Conference on Information Management and Processing (ICIMP 2018)*, pp. 42-48, 2018.

  This paper provides analysis of the outsourcing business practice and identifies its benefits, risks, and all other processes and arrangements associated with it. The content of this paper is covered in Chapter 2 of this research.
- M. Almutairi and S. Riddle, "ISMSs In outsourcing Context," in (*IEEE) 21st Saudi Computer Society National Computer Conference (SCS-NCC'2018)*, 2018.

  This publication provides a review of some of the existing ISMS standards and frameworks that have been reviewed in this research. The paper's content is covered in Chapter 3.
- M. Almutairi and S. Riddle, "Managing Security and Compliance Risks of Outsourced IT Projects", in *Fifth International Conference on Soft Computing (SCOM 2017)*, pp. 33-42, 2017.

  The OSCR framework that has been designed to manage the security and compliance risks of outsourced IT projects is presented in this

paper. The scope of this paper is covered in Chapters 4 and 5 in this research.

- M. Almutairi and S. Riddle, "Security threat classification for outsourced IT projects," in *(IEEE) 11th International Conference on Research Challenges in Information Science (RCIS 2017)*, pp. 447-448, 2017.

  In this paper, the threat classification approach that has been designed for the outsourcing context is presented. The paper's content is covered in Chapters 4 and 5.
- M. Almutairi and S. Riddle, "A Framework for Managing Security Risks of Outsourced IT Projects: An Empirical Study," in (*ACM) the International Conference on Software Engineering and Information Management (ICSIM 2018)*, pp. 40-44, 2018.

  This publication presents the evalution results of the focus group and questionnaire. The scope of this publication is covered in Chapter 6.
- M. Almutairi and S. Riddle, "Managing Outsourced IT Projects Security Risks: A Case Study," in (*ACM) 10th International Conference on Information Management and Engineering (ICIME 2018),* pp. 21-26 2018.

  This publication presents the evalution results of the case study. The scope of this publication is covered in Chapter 7.

1.8 Thesis Structure

This thesis consists of eight chapters. The following describes the thesis chapters briefly:

- **Chapter 1 (Introduction):** The research objectives, questions, methodology, contributions and publications are highlighted in this chapter.

- **Chapter 2 (Background):** It gives background information related to outsourcing business practices as well as discussing their benefits, risks and all other processes and arrangements associated with them.
- **Chapter 3 (Related Work):** It reviews existing ISMS standards and frameworks in the outsourcing context. Their strengths and weaknesses in managing the security and compliance risks of outsourced IT projects are identified.
- **Chapter 4 (Requirements for Managing the Security and Compliance Risks of Outsourced IT Projects):** This chapter discusses the requirements that need to be met in order to manage security and compliance risks effectively when outsourcing.
- **Chapter 5 (Managing the Security and Compliance Risks of Outsourced IT Projects):** The OSCR framework for managing the security and compliance risks of outsourced IT projects is presented in this chapter. It also explains how the OSCR framework tackles the problems and weaknesses of existing ISMS standards and frameworks in addressing outsourcing security requirements.
- **Chapter 6 (Experts Evaluation):** It describes the first evaluation method, which involves a focus group and questionnaire. The evaluation results are presented and analysed in this chapter.
- **Chapter 7 (Case Study):** in this chapter, the OSCR framework is applied to real outsourced IT projects and the results are discussed and analysed.
- **Chapter 8 (Conclusion):** It summarises the research and provides future directions for extending this work.

1.9 Research Definitions

- ***Information System:*** *"A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" [16].*

- ***Information Technology:*** *"Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency" [16].*
- ***IS Outsourcing:*** *"The organizational decision to turn over part or all of an organization's IS functions to external service provider(s) in order for an organization to be able to achieve its goals"* [3].
- ***Information Security:*** *"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" [16].*
- ***Information Security Management System (ISMS):*** *"that part of the overall management system, based on a business-risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" [17].*
- ***Confidentiality:*** *"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" [16].*
- ***Integrity:*** *"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity" [16].*
- ***Availability:*** *"Ensuring timely and reliable access to and use of information" [16].*
- ***Risk:*** *"A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" [16].*
- ***Threat:*** *"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, modification of information, and/or denial of service" [16].

- ***Assets:*** *any project resources (software, hardware, information, etc.) tangible or intangible that represent a value for the project and the organization* [18].
- ***Vulnerability:*** *"A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat" [19].*
- ***Countermeasures:*** *"A technique or a process which helps to achieve one or more security goals and helps to mitigate risks to information and vulnerabilities in an IS"* [20].
- ***Information Security Framework:*** *"is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment" [21]*
- ***Information Security Standard:*** *"documented agreements containing exact criteria that must be followed consistently as rules, guidelines or definitions of characteristics to ensure that any materials, products, processes or services are fit for their purpose" [22]*

Chapter 2 Background

This chapter provides background information related to outsourcing business practices. Before we proceed to the next stages of this research, it is important to understand outsourcing business practices, their benefits and risks, and all other processes and arrangements associated with them. This will allow us to identify outsourcing security issues and needs for managing the security and compliance risks of outsourced IT projects.

2.1 Introduction

As a result of globalisation and heightened competition, many organisations today find it difficult to develop services that satisfy customers' needs; these needs need to be met on time, despite the organisation's resource limits, so that the organisation can compete effectively [23]. With the emergence of cloud computing, and advancements in web technology, challenges and customers' demands increase. Hence, organisations recognise the need to consider potential alternatives that help them to meet such tremendous demands and improve their agility [24].

In response to these challenges and demands, many organisations consider outsourcing as a choice for delivering and improving their Information Technology (IT) services. Over the last two decades, Information Systems (IS) outsourcing has grown rapidly. Indeed, this growth has attracted academia and industry to investigate the outsourcing benefits that organisations could gain from outsourcing, as well as the outsourcing risks that might be encountered and which should be avoided when adopting such a choice.

The rest of this chapter is structured as follows: we discuss the types of outsourcing arrangements in Section 2.2. We highlight the outsourcing process in Section 2.3, and we discuss outsourcing benefits and risks in Sections 2.4 and 2.5 respectively. In Section 2.6, we present security issues with outsourcing. In

Section 2.7, outsourcing security needs are presented. We summarise this chapter in Section 2.8.

2.2 Outsourcing Arrangement

Outsourcing arrangements can be categorised into four types [4]: general outsourcing, transitional outsourcing, business process outsourcing, and business benefit contracting. These types are summarised as follows:

2.2.1 General Outsourcing

This type of outsourcing has three possibilities:

2.2.1.1 Selective outsourcing

The organisation chooses one area from its information system functions to be run by a third party, such as disaster recovery (DR) operations. The decision to outsource any specific area should be aligned with the organisation's strategic plan, and return the expected value to the organisation [4, 25].

2.2.1.2 Value-added outsourcing

Some areas of information system functions are carried out by a third party who is believed to add higher value to the service or support, and which cannot be achieved by the organisation at an appropriate cost [4, 26].

2.2.1.3 Co-operative outsourcing

The organisation and the third party co-operate jointly to perform specific tasks in the organisation's information system [27]. The organisation benefits from the third party's skills and knowledge and these tasks are performed effectively. As a result of such joint cooperation, the third party's knowledge and skills will be transferred to the organisation's staff [4].

2.2.2 Transitional Outsourcing

In this option, the organisation decides to replace their technical platform by another one through a third party. This replacement might be due to a new technology need, cost reductions, or any other reasons [4, 28]. It involves three phases:

- Legacy system management.
- New technology management.
- New platform management and stabilisation.

2.2.3 Business Process Outsourcing

In this option, a third party runs all the functions of the business on behalf of the organisation [4, 29]. Although this option is relatively new, many organisations consider it as a new opportunity to gain more benefits and compete effectively. Examples of this option may include call centres, help desks, and document processing functions.

2.2.4 Business Benefit Contracting

In this option of an outsourcing arrangement, an organisation seeks specific business benefits, which they believe will be delivered effectively by a third-party provider. The organisation subcontracts with the third party, and defines the business benefits that the third party will achieve for the organisation in a specific period of time. Moreover, it defines the organisation's way of paying the third party when the agreed business benefits have been achieved. The rationale behind this option is to match the cost being paid with the benefits being received. However, this option is not widely adopted. The main reasons for not adopting this option are the difficulties in measuring agreed benefits, and the uncertain revenue for the provider that is associated with this specific option of outsourcing [4].

2.3 Outsourcing Process

Outsourcing involves creating and managing a contractual agreement between an organisation and a third party. This process defines the services and obligations that both parties should achieve through this relationship. Despite the difficulty of identifying an accurate outsourcing process category that reflects the actual practice of the outsourcing process, a great deal of work has been done by researchers to categorise the outsourcing process. Some researchers have elaborated and proposed a very detailed outsourcing process, whereas others have proposed a very limited outsourcing process. The authors in [30] and [31] propose six phases for the outsourcing process. Each phase has many detailed activities. On the other hand, the authors in [32] propose three phases for the outsourcing process. Other authors have proposed five phases [33].

Despite the differences in defining an accurate outsourcing process, the outsourcing process encompasses four major phases. Those phases are Planning, Implementation, Operation, and Closing. Each phase consists of different activities. The four phases are summarised as follows [33]:

2.3.1 Planning Phase

At this phase, the organisation should explore and validate the reasons that make outsourcing an appropriate option. Expected benefits and possible alternatives should be identified and analysed, as well as the strategy being used in the outsourcing process. Vendors are evaluated using specific criteria set by the organisation at this phase too. The aim of this evaluation is to select the appropriate provider. Vendors' evaluation is based on their responses to the Request For Proposal (RFP) issued by the organisation. Other factors may influence the result of the evaluation, such as the budget allocated to the project. Moreover, this phase involves contract negotiation and signing with the selected vendor. By the end of this phase, answers to the following questions should have been clearly identified: What to outsource? To whom to outsource?

2.3.2 Implementation Phase

Having answered the question about who to outsource to, and having signed the contract with the selected vendor, the services planned at the previous phase are put into practice. Human resources adjustment and communication management, in addition to relationship management, are carried out at this phase too. The relationship between the two parties involved in the outsourcing process (the vendor and the organisation) is controlled through the contract. A successful relationship relies on the way that both parties manage the relationship.

2.3.3 Operation Phase

At this phase, the services that have been developed at the implementation phase are operated and monitored by the provider. Any issues or defects are analysed and fixed in order to meet the organisation's requirements.

2.3.4 Closing Phase

At this phase, the organisation evaluates the outsourcing relationship in terms of the benefits that have been achieved, and it analyses the lessons learned. Moreover, the organisation should assess whether to extend this contract or not, and what process changes need to be implemented for this contract or any other contracts in order to gain the greatest possible benefits. Although this phase is usually carried out just before the contract ends, it might be carried out at any time of the contract, especially when there are some indicators that might affect the contract, such as contract violations by the vendor.

2.4 Outsourcing Benefits

Although the development of information system services can be seen as the responsibility of the organisation's computing department in general, different organisations adopt IS outsourcing because it provides many economic benefits,

in a business world where competition can increase rapidly [26, 34, 35]. Such benefits have increased the popularity of outsourcing, not only in IT organisations, but in different types of businesses such as financial firms, call centres and insurance firms [36]. Those benefits that may lead to outsourcing information system functions either partially or totally are summarised as follows:

2.4.1 Cost Reduction

The financial factor is one of the major factors that has strongly influenced IS outsourcing. By outsourcing some of their IS functions, organisations have access to the providers' qualified experts. Hence, organisations neither need to hire IT consultants for a long time to run some IS functions that require some expertise, nor do they need training programmes, which add extra costs [34]. As a result, the organisation will have the ability to reallocate its key personnel to core business functions, which usually are not outsourced. Such reallocation could enhance productivity and increase the overall profit [6].

2.4.2 Enable Concentration on Core Business Activities

Many organisations experience difficulties in focusing on all business activities and achieving excellence across the board when delivering services to their customers. When focusing on all business activities, an organisation's personnel are made responsible for achieving all of the organisational goals, whether they are strategic or not, which might overload them and negatively affect their creativity. Hence, outsourcing non-strategic activities could help organisations to focus on their core strategic activities, rather than concentrating on all of them at the same time, which might consume the organisation's resources and result in a loss of competences. Organisation executives should decide what will be considered as a core activity for the business and what will be not. All activities that contribute to the success of the business (normally carried out internally) are widely considered as core business activities. Moreover, activities that might add a high value to the organisation, for example enabling it

to compete effectively or affecting its growth, should be considered core activities as well [37].

2.4.3 Flexibility Improvement

The enormous changes in IT that have resulted from the rapid advancements in this field add extra challenges to organisations. Responding to these changes may require a great deal of investment by organisations to upgrade their IS and to obtain the required support to run and maintain the upgraded part of the system. Although organisations may vary in their responses to upgrading their IS with the latest technology, upgrading gives organisations the ability to access new resources. This in turn might improve their agility and their ability to provide their customers with competitive services. Outsourcing could help organisations to deal with such challenges. Organisations may design their third parties' contracts so that they respond properly to these changes and meet their IT needs. However, changes are not only experienced in IT; customer needs are also continuously changing. Different organisations consider outsourcing as a business practice that helps to improve their response to business changes and customers' needs [38].

2.4.4 Quality Improvement

Quality of services is one of the reasons why organisations decide to outsource some of their information system functions. Many organisations consider delivering high-quality services to their customers an important element of creating a good reputation. Therefore, when outsourcing, third parties should provide services that are higher in quality than those that have been achieved previously by the organisation [8, 39]. Providers may be able to achieve higher quality services for a number of reasons. One reason is that most providers are specialised in specific IT areas, such as software development, or one specific technology such as cloud computing. This specialisation means that they have spent a long time working in that specific IT area, and they have therefore gained a great deal of relevant skills, which enable them to perform their tasks

effectively. Training programmes that providers offer to their staff could also improve their efficiency in delivering high-quality services. Another reason is that providers have more access to new technologies, which afford them advantages in managing their tasks. This could contribute to improving coordination and control, and it motivates staff to do their jobs effectively.

2.4.5 Minimising Routine Tasks

Being able to concentrate on strategic activities is a major success factor in any organisation that needs to compete effectively. Although many organisations have their own information system experts, they are not utilised in a way that promotes competiveness. Experts are influenced by routine tasks such as system maintenance operations. Routine tasks may take much of their time and probably do not add much value to the organisation. To avoid overloading information system experts, many organisations have realised that experts should focus only on tasks that add higher value to the organisation. Different organisations have turned over their routine tasks to third-party providers in an effort to focus on core business activities that create competitive value for the organisation. Consequently, greater efficiency can be achieved as deeper knowledge can be gained through specific training as a result of this concentration. This enhances organisations' ability to deliver better services to their customers with lower costs [40].

2.4.6 Minimising the Obsolescence Risk

The risk of technology obsolescence is another reason why organisations decide to outsource some of their information system activities. The rapid advancement of IT leaves organisations with two options. The first one is to invest in their IT more often, in order to access the latest technology, which could help to improve the services they deliver to their customers. Consequently, this will increase the cost of their information system and affect their overall profit. The second option is to continue using their current information system with minimal upgrades to the latest technologies. However, this option is not even

beneficial. The organisation will miss the opportunity to access the latest technologies, which could have improved their ability to deliver better services at a lower cost. Organisations may encounter extra expenditures when mandatory new technology is implemented, for example training programmes will be required for staff to refresh their knowledge and skills. Outsourcing could provide an appropriate solution for these difficulties. If contracts with third parties are designed properly, organisations could access the latest technologies and be relieved from the obsolescence risk, as it will be the provider's responsibility [1].

2.5 Outsourcing Risks

Although outsourcing is becoming widespread among different organisations due to the benefits that it can provide, it is also associated with different risks that need to be addressed and managed properly, otherwise they could lead to major failures, not only in one particular project, but over the entire organisation [11]. Some organisations might overstate the benefits that third parties can achieve at the beginning of projects, which improves their first impressions. The benefits achieved early on may lead to the organisation neglecting risk management and failing to control identified risks throughout the project. As a result, some of these identified risks may become reality, seriously affecting the expected benefits from outsourcing. In the literature, researchers have identified different risks associated with outsourcing. Those risks are summarised as follows:

2.5.1 Security Risks

Confidentiality, which refers to protecting information from being disclosed to unauthorised users, is a major security issue [41]. The issue of confidentiality in outsourced projects arises from the nature of the work carried out by third-party providers. They are more likely to discover clients' business secrets related to financial affairs, services or technologies, as they work with different organisations. Disclosing business secretes, intentionally or by mistake, may result in real consequences for the organisation, such as a loss of competences or

reputation [42]. Organisations that intend to outsource some of their information system functions should consider this risk seriously before starting any outsourced project. Decisions about security policies, in addition to security controls that fulfil confidentiality criteria, should be taken by the organisation itself. Technical aspects that protect confidentiality could additionally contribute to minimising this risk. Relying only on security polices and technical security controls might be not enough to protect confidentiality. Such drawbacks might be mitigated by Non-Disclosure Agreements (NDAs), comprehensive Service Level Agreements (SLAs), and contract terms [43].

2.5.2 Contract Violations

Outsourcing with a third-party provider is intended to achieve particular requirements. When an organisation takes the decision to outsource some or all of its information system functions, all of the requirements for this project are identified and announced in the Request For Proposal (RFP) document that organisations usually use in outsourcing projects. Providers use this RFP to respond to the organisation's requirements and to propose solutions that meet these requirements. Nevertheless, not all RFPs are written in a way that providers can discern the requirements accurately. Therefore, contract violation issues may arise from a lack of clarity over the project requirements in the client's RFP. This might affect the preferred provider's (the winner's) ability to meet the project requirements as expected [44].

Misunderstanding project requirements is not the only reason for contract violation. Other reasons may contribute to this issue. Some providers may propose ideal solutions with reasonable costs that suit the project budget allocated by the organisation. Nevertheless, when the provider executes the project, the organisation realises that the solutions being executed do not match what has been proposed, whether in a small or a large way. This difference may stem from the provider's plan to reduce costs in order to increase its overall profit; or it might stem from the provider's inability to achieve what has been proposed due to insufficient technical experts.

2.5.3 Loss of Technology Skills

The issue of losing technology knowledge and skills is another issue that might be encountered by organisations when outsourcing some of their information system functions. In outsourcing, most services are delivered by the provider without any participation from the organisation's staff. Non-participation in the development and delivery of services will gradually lead to a dependency on the provider's staff for these particular services. By the end of the contract, the organisation may realise that the required technical skills and knowledge to run such services have not been gained by its staff. Hence, the organisation needs to consider this issue carefully before entering any outsourced contract, in order to avoid any technical dependency. Both parties, the organisation and the provider, need to work together to develop a knowledge transfer plan for technical skills. This will allow the organisation's personnel to be technically able to run these services when the contract ends. The plan should be put into practice at the early stages of the project's execution and it should be monitored carefully to ensure that it achieves its aim. Nevertheless, core services should be kept inside the organisation to avoid any loss of capability to innovate services that allow the organisation to compete effectively [45].

2.5.4 Inadequate Provider Qualifications

Many organisations consider outsourcing as an appropriate solution to access the latest technologies and to employ technical experts at an appropriate cost. Nevertheless, not all providers meet organisations' expectations in this regard [46]. Different reasons may contribute to this issue, although there are some variations between providers. The issue might arise at the early stages of the project's execution as some providers want to find staff who have a good background in the client's information system and its infrastructure. Those staff will transfer the required knowledge to the provider's staff and participate in delivering services to the client. Previous qualified staff of the client could add a high value to the project, but that is not always the case. The problem arises when unqualified staff are hired for developing and delivering services to the

client. As a result, the client finds that its unqualified staff are working on its project.

This risk also may arise when a provider has many projects with limited key personnel. The provider may move key personnel to another important project or may allocate them to achieve some tasks for a short time with each project. As a result, key personnel may lose their concentration and ability to develop innovative services.

2.5.5 Hidden Costs

Cost reduction is one of the main drivers for organisations to outsource their information system functions partially or totally. However, many organisations may realise that this benefit is not effectively achieved. This may be due to a failure to accurately estimate the overall cost when deciding to outsource some functions to a provider. These estimates usually take into account only the expected cost of delivering particular services requested by the organisation. They should, however, take into account other factors that affect the overall cost of the outsourcing. This includes costs encountered by the organisation when looking for and evaluating different providers, in order to select the most suitable provider for the organisation. Additionally, at the beginning of the project, the provider's staff need to have some sort of knowledge transfer to ease their understanding of the client's IS. Knowledge transfer is conducted by the client's staff and the cost of this process should be included when estimating the overall project budget. The other costs that should be included are the costs of overseeing the project and the provider's staff, and the costs involved with managing the contract. If the organisation understands the real cost of outsourcing, it can more accurately assess and decide whether to outsource or not, and avoid hidden costs [47].

Table 2.1 provides a summary of the benefits and risks of outsourcing that have been presented in this chapter.

Table 2.1: Outsourcing Benefits and Risks Summary

Outsourcing Benefits	Outsourcing Risks
Cost Reduction	Security Risks
Concentration on Core Business Activities	Contract Violations
Flexibility Improvement	Loss of Technology Skills
Quality Improvement	Inadequate Provider Qualifications
Minimising Routine Tasks	Hidden Costs
Minimising the Obsolescence Risk	

2.6 Outsourcing Security Issues

Despite the fast growth of outsourcing, there are particular security issues that need to be analysed and monitored by organisations to mitigate their potential impact. Several studies have identified a great deal of security issues with outsourcing [2, 12, 48-50]. However, providing a complete list of outsourcing security issues seems to be difficult for several reasons (e.g. technology changes, level of IS complexity, etc.). Instead, security issues can be broadly classified into four categories [2, 48, 49]: organisational, technical, human, and physical and environmental. The following sub-sections provide more details about these categories and offer examples of security issues related to these four categories.

2.6.1 Organisational Security Issues

This category represents issues related to the security practices of the organisation (the client) or the provider. The following are examples of security issues belonging to this category:

- Lack of security policies and procedures.
- Lack of clarity of security requirements.
- Lack of or inadequate asset management.
- Lack of clarity in contract conditions between the two parties (the client and provider).

2.6.2 Technical Security Issues

This category involves issues that might arise due to technical issues. Examples of technical security issues include:

- Software application bugs.
- Improper firewall configuration.
- Improper user event log.
- Lack of intrusion detection system.

2.6.3 Human Security Issues

This category represents security issues that might arise due to human issues. The following provides some examples of human security issues:

- Lack of security awareness.
- Absence of NDA.
- Human errors.

2.6.4 Physical and Environmental Security Issues

In this category, issues related to physical and environmental conditions are involved. Examples of these issues include:

- Lack of temperature controlled system.
- Lack of fire resistance system.
- Lack of physical access control.

2.7 Outsourcing Security Needs

As the growth of outsourcing rapidly increases, ISs become more complex and involve different entities. Outsourcing is not always beneficial; security risks are associated with it, such as confidentiality, compliance, availability of services and so on. It is understood that IT outsourcing might face same traditional security risks [51]. However, when it comes to managing the security and compliance

risks of outsourced IT projects effectively, a comprehensive methodology should be in place. This should address all potential security risks of IT outsourcing and propose effective security controls that mitigate their impact. The lack of such a methodology raises the question of whether or not the existing methodologies are applicable for the outsourcing context [12]. Before answering this question, particular outsourcing security needs should be determined, in order to assess the applicability of the existing methodologies in the outsourcing context. The following highlights the security needs for the outsourcing context [52-55]:

- Security requirements management: the security programme or framework should be comprehensive and systematic as well as establishing a complete methodology that is capable of adequately managing the security requirements of outsourced IT projects. This includes information security policies, communications and operations management, access controls, IS acquisition, development, and maintenance, asset management, incident management and business continuity management.
- Risk Management: Security risks are not only technical; therefore, the security programme should manage risks from different perspectives such as technical, human, and environmental and physical risks.
- Consideration of Outsourced IT Projects: to mitigate the security risks of outsourced IT projects, the ISMS should establish a method that takes into consideration the outsourcing context.
- Compliance management: The security programme should establish a method to enforce compliance properly.
- Usability: The security program should be usable in the outsourcing context from different perspectives such as cost effectiveness, time efficiency and simplicity.

2.8 Summary

IS plays a major role in the modern businesses of most organisations. Although developing and maintaining the IS are traditionally seen as the

organisation's responsibility, many organisations consider outsourcing to be an attractive alternative.

Outsourcing can be categorised into four types: general outsourcing, transitional outsourcing, business process outsourcing, and business benefit contracting. The outsourcing process encompasses four major phases: Planning, Implementation, Operation, and Closing. Each phase consists of different activities.

Different benefits can be gained from outsourcing. Cost reductions, concentration on core business activities, flexibility and quality improvement, and minimising routine tasks and the obsolescence risk, are just some examples of these benefits. Despite the enormous benefits that outsourcing can offer organisations, it might expose organisations to different risks such as security risks, contract violations, loss of technology skills and hidden costs.

Previous studies have identified a great deal of security issues in outsourcing. For several reasons (e.g. assets involved, security practices of both parties, etc.), providing a complete list of outsourcing security issues seems to be difficult. To overcome this difficulty, security issues can be broadly classified into four categories: organisational, technical, human, and physical and environmental.

To manage the security risks of outsourcing effectively, organisations need to take into account several elements that aim to improve the overall security management of the organisation. The security program or framework should embrace different features such as establishing a comprehensive methodology for managing security requirements, managing security risks from different perspectives, managing compliance, and being usable from different perspectives such as cost effectiveness, time efficiency and simplicity.

In the following chapter, existing Information Security Management System (ISMS) standards and frameworks will be reviewed to assess their applicability to managing the security and compliance risks of outsourced IT projects.

Chapter 3 Related Work

The previous chapter gives background information about outsourcing business practice. This chapter reviews existing Information Security Management System (ISMS) standards and frameworks to investigate their ability to manage the security and compliance risks associated with outsourced IT projects. Based on this review, their focus, strengths and limitations in managing the security and compliance risks of outsourced IT projects can be identified.

3.1 Introduction

In modern business, where organisations are heavily dependent on their IS, information security become a key challenge, as it requires a great deal of knowledge not only about technical aspects, but also about people and environmental aspects [56]. Organisations have realised the importance of ISMS standards and frameworks in managing the security risks of their information systems; they are a key element of their strategy to overcome information security challenges [57]. The selection and implementation of an ISMS standard or framework should therefore provide a level of protection that mitigates the impact of any potential security risks. However, the selection of the ISMS should be made based on a deep analysis of the security threats that exist in the organisation [58]. It should also provide the required protection for information security key characteristics, e.g. confidentiality, integrity and availability [54].

Another key element in overcoming information security challenges is enforcing compliance with the chosen ISMS standard or framework. Indeed, it is true to say that compliance enforcement has become as valuable as the adoption of the security standards and frameworks, which are implemented to achieve organisations' security objectives [59]. Otherwise, ISMS standards and frameworks might not achieve the security goals expected by the organisation [60]. Compliance enforcement ensures that ISMS standards and frameworks can work effectively to provide the required information system protection [61, 62].

The rest of this chapter is structured as follows: we discuss existing ISMS standards and frameworks in Section 3.2. We evaluate the identified ISMS standards and frameworks in Section 3.3. Finally, we summarise this chapter in Section 3.4.

3.2 Existing ISMS Standards and Frameworks

Different ISMS standards and frameworks have been developed for managing the security risks of information systems. These ISMS standards and frameworks may have some similarities or differences, based on the steps or procedures that they follow to achieve the security objectives of organisations. In order to identify suitable candidates from the existing ISMS standards and frameworks, we first classify them into four themes based on their focus [63-66]: Information Security Management, IT Governance and Service Management, Risk Management, and Security Architecture and Engineering. Each theme is then presented by representative examples. These ISMS representative examples have been chosen due to their ability to manage security risks. We tried to include only the leading standards and frameworks [63, 67-71] in each theme as representative examples. They are expected to help with managing the security risks of outsourced IT projects, as they are dedicated to the management of security risks partially or totally.

3.2.1 Information Security Management

This theme comprises systematic ISMS standards and frameworks that describe rules, processes, and procedures with regard to information security within an organisation. They try to explain how to protect an information system as a central asset of the organisation in the form of best practices or guidelines. The following are examples of standards and frameworks within the information security management theme:

3.2.1.1 ISO/IEC 2700x series

One of the most adopted ISMS is ISO/IEC 2700x series. It was originally developed by the UK National Computing Centre (NCC) in 1993. The first publication was *"PD 0003 A Code of Practice for Information Security Management"*. Two years later, the work was adopted by the British Standards Institute (BSI) and *"BS 7799-1 IT—Security Techniques—Code of Practice for Information Security Management"* was published as a national standard. Later on, the work was complemented by *"BS 7799-2 Information Security Management Systems—Specification with guidance for use"* [72]. In 2000, BS7799-1 was accepted and published by the International Standards Organisation (ISO) and the International Electro-technical Commission (IEC) as the ISO/IEC 17799 standard. Later on, ISO/IEC 17799 was renumbered to ISO/IEC 27002 and BS 7799-2 became ISO/IEC 27001 standard [70]. Figure 3.1 shows the development history of the ISO/IEC 2700x.

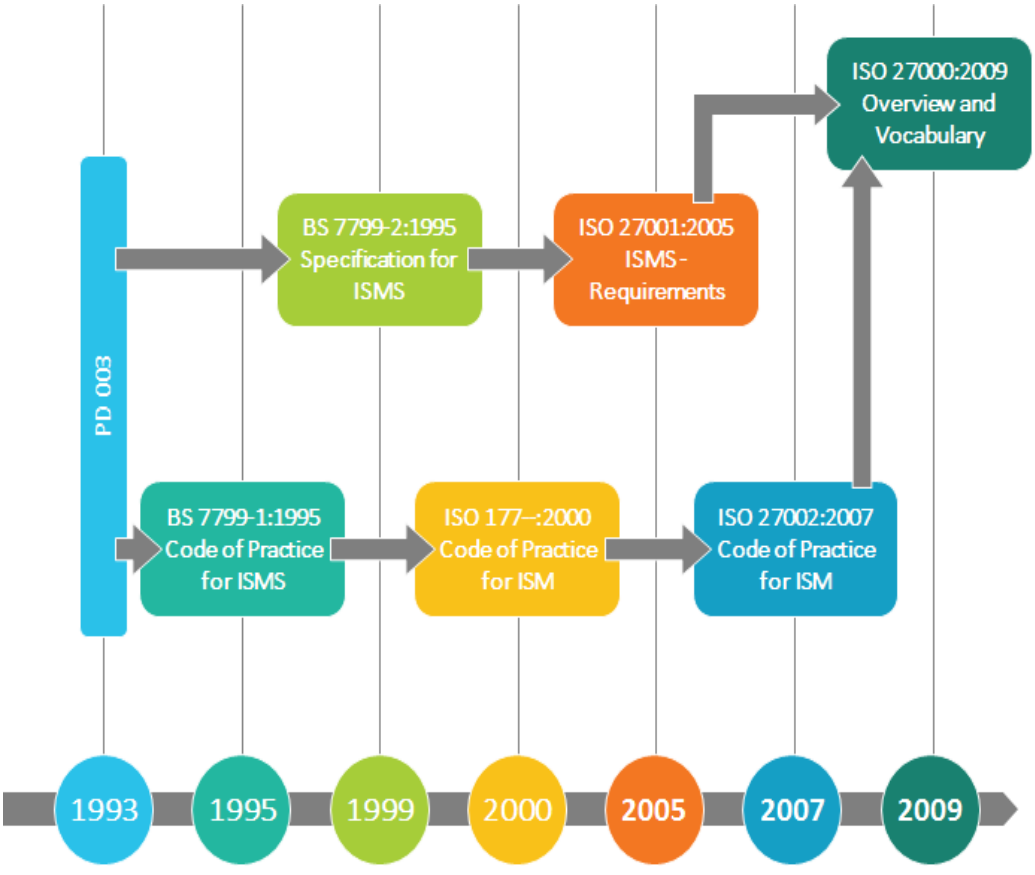

Figure 3.1: Development History of ISO/IEC 2700x [72]

The following highlights the most relevant ISO/IEC 2700x series publications:

- **ISO/IEC 27000:** This publication provides an overview of the vocabulary, terms, and definitions of ISMS. It outlines other ISO/IEC standards covered in this series. The fundamental and basic security knowledge that organisations should know are covered in this standard too [73].
- **ISO/IEC 27001:** The ISO/IEC 27001 provides organisations with guidance on how to design, implement and operate their ISMS. This standard is based on the Plan-Do-Check-Act (PDCA) model, which provides continuous improvement. The security requirement specifications provided in this standard are used as the basis for certifying organisations with ISO/IEC 27001 [74-76].
- **ISO/IEC 27002:** This standard provides a set of best practice security controls that are intended to achieve security requirements' specifications proposed in the ISO/IEC 27001 standard. Those controls are optional and organisations could use their own controls as long as they achieve the security requirements' specifications effectively. The ISO/IEC 27002 standard recommends 114 controls grouped into 14 domains that could help organisations with achieving their security goals [77, 78].
- **ISO/IEC 27003:** This standard provides guidance on how to plan and implement a practical ISMS based on the security requirements' specifications provided in ISO27001. The standard provides support to deal with critical activities at the early stages of ISMS implementation. It does not cover operational activities resulting from ISMS implementation [79].
- **ISO/IEC 27004:** This standard provides guidance on how to use measures to evaluate the effectiveness of organisations' ISMSs according to ISO/IEC 27001 specifications. The results of this evaluation help organisations identify processes and controls that need to be changed or improved [70, 80].

- **ISO/IEC 27005:** This standard provides guidance for information security risk management in accordance with ISO/IEC 27001. This standard does not follow any specific risk management methodology. It is the responsibility of organisations to establish or choose their risk management methodology that suits their contexts [70, 81, 82].

3.2.1.2 NIST SP 800- series

The National Institute of Standards and Technology (NIST) has developed a series of standards and guidelines about information security for federal agencies. The special publications (SP) of these guidelines cover different topics of information security, such as security plans and risk assessment. These standards and guidelines represent the minimum requirements for securing the IS of federal agencies. The following outline the most relevant NIST standards and guidelines:

- **NIST SP 800-18:** This special publication of NIST provides guidance on how to develop a security plan for federal systems. The minimum requirements that should be covered by the security plan include information system name, purpose, categorisation, owner, type, environment, and status. Moreover, the security plan should list any integration with other systems, identify any related regulations or policies, and choose appropriate security controls [83, 84].
- **NIST SP 800-30:** This document provides guidance on how to conduct the risk assessment of federal systems. It starts by describing the process of risk assessment and the terminologies used for assessing information system risks. Moreover, the document describes the activities required before conducting risk assessment, the activities required to carry out risk assessment, and the activities required for producing risk assessment results [85, 86].
- **NIST SP 800-34:** This document provides guidance on how to develop contingency plans. Different types of plans are discussed in this document, including business and operations continuity, crisis

communications, disaster recovery, critical infrastructure protection, and cyber incident response plans. Seven steps are identified for developing appropriate contingency plans. Those seven steps are:

- Develop the contingency planning policy statement.
- Conduct the business impact analysis (BIA).
- Identify preventive controls.
- Create contingency strategies.
- Develop an information system contingency plan.
- Ensure plan testing, training, and exercises.
- Ensure plan maintenance.

The document provides recommendations about contingency plans for three types of platforms: client/server, telecommunications and mainframe [87].

- **NIST SP 800-53:** This document proposes a catalogue of security and privacy controls that can be adopted by federal systems and organisations. It also explains the process of selecting appropriate controls that help to protect an organisation's IS from different security and privacy risks. The selection of appropriate controls is based on the risk assessment that is conducted by organisations before implementing any security or privacy controls. The proposed controls are comprehensive and customisable to meet different business types and missions. Those controls address security from two perspectives: functionality and assurance [88, 89].
- **NIST SP 800-55:** This document provides guidance on how to develop and implement appropriate measures that assist organisations in assessing the effectiveness of their chosen security controls. Those measures should identify any performance issues related to the security program, and provide appropriate corrective actions that need to be implemented to resolve these performance issues [90, 91].
- **NIST SP 800-137:** This document provides guidance on how to develop and implement a strategy for information security continuous monitoring of federal systems and organisations. The aim of this

continuous monitoring is to enhance the awareness of vulnerabilities and threats associated with IS. A robust continuous monitoring strategy should be comprehensive, and should take into account different factors such as technology, environment, people and processes [92].

3.2.1.3 GMITS (ISO/IEC 13335)

The Guidelines for the Management of IT Security (GMITS), known also as ISO/IEC 13335, is a comprehensive programme for managing IT security. It has been developed by the ISO and the International Electro-technical Commission (IEC). GMITS manages IT security from different perspectives such as technical, physical, and managerial. It is grouped into five parts. The first part, called *Concepts and Models for Information and Communications Technology Security Management*, describes the basic definitions, concepts and models that need to be understood by managers responsible for the organisation's overall IT security programme. The second part, known as *Managing and Planning IT Security*, covers aspects related to managing and planning an effective security programme. It targets managers involved in designing and overseeing the organisation's security programme. The third part, called *Techniques for the Management of Information Technology Security*, describes security risk approaches that can be used by those involved in assessing IT security risks. The fourth part, called *Selection of Safeguards*, provides guidance on how to choose appropriate safeguards that help to reduce IT security risks. The fifth part, called *Management Guidance on Network Security*, provides guidance on how to address the security requirements of networks and communications when using external or public communications [93, 94].

3.2.2 IT Governance and Service Management

This theme includes ISMS standards and frameworks that provide a governance or methodology for implementing processes, structures and relationships. These enable IT and business strategy administrators to execute

their responsibilities with regard to achieving the expected business values [95]. The following are examples of standards and frameworks within this theme:

3.2.2.1 COBIT

The Control Objectives for Information and related Technology (COBIT) is a comprehensive framework that was developed by an international professional association called the Information Systems Audit and Control Association (ISACA) in 1996. Its aim was to help enterprises to achieve optimal values from their IT by balancing benefits realisation, and optimising risk levels and the use of resources. The framework consists of a set of best practices for IT governance and management that have evolved over the last two decades [96, 97].

The latest version, COBIT 5, has five principles and seven enablers, as shown in Figure 3.2 and Figure 3.3 respectively. The two domains that are covered are governance and management. The governance domain consists of five processes whereas the management domain has 32 processes. Those processes act as guidance for enterprises that intend to implement COBIT 5 [98].

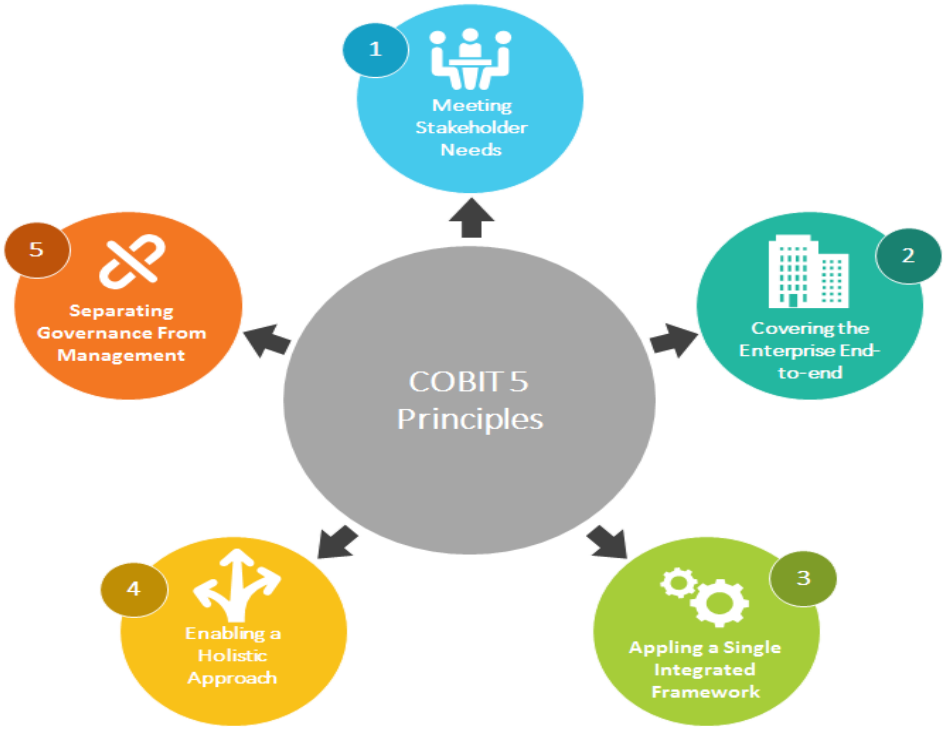

Figure 3.2: COBIT Principles [99]

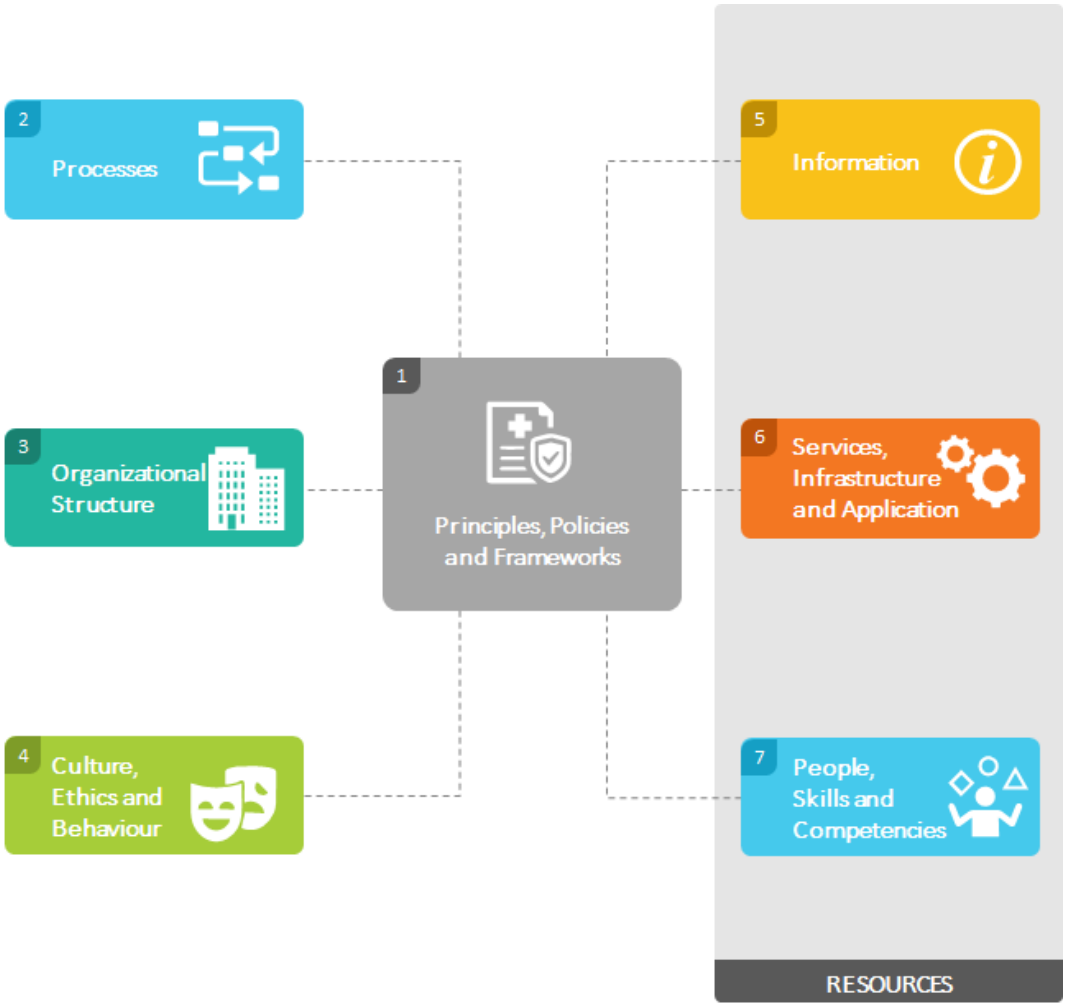

Figure 3.3: COBIT Enablers [99]

3.2.2.2 ITIL

The Information Technology and Infrastructure Library (ITIL) framework has been developed by the UK government's Office of Government Commerce (OGC) for IT service management. The framework is a set of best practices that can be used to improve enterprises' performance in managing their IT services [100, 101]. Different benefits can be achieved by using the ITIL framework, such as cost reductions, IT service improvement, and IT services aligned with the enterprise's business needs [102]. ITIL has been developed to cover the lifecycle of a service, which has five stages: Service strategy, Service design, Service transition, Service operation, and Continual service improvement [103]. Those stages are presented in Figure 3.4 and summarised as follows:

Figure 3.4: ITIL Lifecycle Stages [103]

- Service Strategy: at this stage of a service lifecycle [104], the framework provides guidance on how to design, manage and operate services that satisfy customers' needs and are in line with the enterprise's IT capabilities and resources. The core topics at this stage include market establishment for the enterprise services, services' assets, and ITIL implementation strategy for the lifecycle of the services. Basic principles of IT service management such as concepts, processes, and references are presented at this stage.
- Service Design: at this stage [105], the framework provides guidance for designing, developing, and managing IT services effectively. Processes and methods that help with transferring enterprises'

strategic objectives into services' portfolios and assets are covered at this stage. Core topics of the Service Design Stage include: improvements and changes of services that lead to increasing customer satisfaction, service continuity, and service compliance with standards and regulations.

- Service Transition: at this stage [106], the framework provides guidance on how to implement strategic services that have been designed and tested. The expected values of the services are realised at this stage. Configuration management and knowledge management are examples of the topics covered at this stage.
- Service Operation: at this stage [107], the framework provides guidance on how to manage services' daily operations. This includes managing performance levels so that they meet customers' requirements, resolving service issues that might arise, and handling customers' new requests. Event, incident and access management are examples of processes that are covered at this stage
- Continual Service Improvement: at this stage of the lifecycle of a service [108], the framework provides principles and methods that help to improve service quality. Moreover, it guides enterprises on how to measure processes' efficiency and effectiveness in order to meet customers' expectations. Mechanisms for managing incremental changes and improvement are covered at this stage as well.

3.2.3 Risk Management

This theme encompasses risk management methods that can be used by organisations to identify and assess the security risks of their IS. The following are examples of standards and frameworks within this theme:

3.2.3.1 OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a self-directed approach for evaluating the security risks associated

with the existing security practices and processes of an organisation. It was developed by Carnegie Mellon University in 1999. The approach does not concentrate on technological risks only, but takes into account other risks such as strategic and security practices. The evaluation is conducted by a small team from different units of the organisation, including IT, business and operations departments. The result of this evaluation is the identification of the organisation's security needs from three balanced perspectives: operational risks, security practices, and technological perspectives [109, 110].

The OCTAVE approach consists of three phases [109, 111, 112]: Build Asset-Based Threat Profile, Identify Infrastructure Vulnerabilities, and Develop Security Strategy and Plan. Those phases, as shown in Figure 3.5, are summarised as follows:

- Build Asset-Based Threat Profile phase: at this phase, the evaluation team identifies assets that are important to the organisation, and evaluates the security practices being used to secure them. Following that, the team selects the organisation's most critical assets and identifies the security requirements for each one of them. At the end, a threats profile is created based on each asset threat. This phase is considered as an evaluation at organisational level.
- Identify Infrastructure Vulnerabilities phase: at this phase, the evaluation team assesses the organisation's technical infrastructure components in order to identify any possible access paths to critical assets that might expose them to security risks. This phase is considered to be an information infrastructure evaluation.
- Develop Security Strategy and Plan phase: at this phase, risks associated with critical assets are identified by the evaluation team. Based on that, the evaluation team develops a strategy plan for protecting the organisation's critical assets from identified risks.

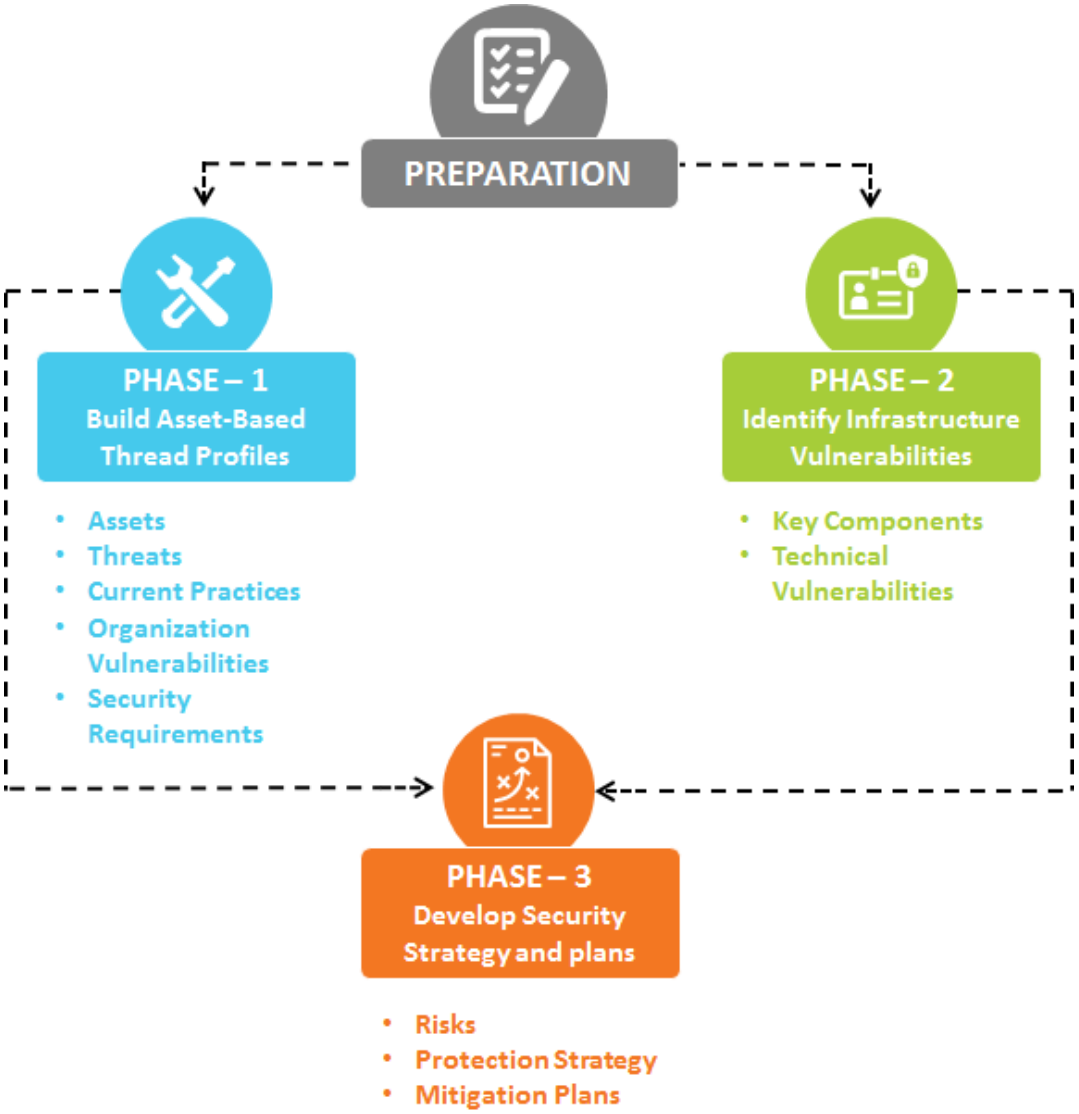

Figure 3.5: OCTAVE Phases [113]

3.2.3.2 CORAS

CORAS is a qualitative model-based approach designed for security risk analysis. It was developed under the Information Society Technologies (IST) programme. It is a European research and technological development project that resulted in a security risk framework (CORAS). It uses the Unified Modelling Language (UML) to model the security risks of critical systems [114, 115]. CORAS uses eight steps for conducting security risk analysis as summarised in the following steps [116, 117]:

- Step 1: This initial step (preparation step) is used to identify the target and the size of the risk analysis.
- Step 2: The second step involves an introductory meeting with the customer the analysis will be conducted for. The aim is to obtain the overall goals of the security analysis and the most important concerns that need to be analysed. By the end of this step, the overall goals, focus, scope and plans for the security analysis are identified.
- Step 3: The third step ensures a common understanding of the outcomes from step 2 between the team and the customer. The overall goals, along with their focus and scope, are finalised. The main assets that need to be protected, the major threat scenarios, and vulnerabilities are identified at the end of this step.
- Step 4: in this step, the customer ensures that the overall goals, scope and focus are complete and correct. Assumptions and preconditions are made. The targets are modelled using UML and the risk evaluation criteria for each asset are identified at the end of this step.
- Step 5: this step is called the risk identification step and it is carried out as a structured brainstorming by analysts. The outcome of this step involves identifications of threats, unwanted incidents, threat scenarios and vulnerabilities for all assets that have been identified.
- Step 6: in this step, the risk level is determined by estimating the likelihood and consequences of the identified risks.
- Step 7: in this step, the risk evaluation criteria are used to decide whether the identified risks are acceptable or not. If not, further evaluation for possible treatment is conducted.
- Step 8: in this step, the risks that are found to need more treatment are analysed in order to reduce their likelihood and/or consequences.

3.2.3.3 CRAMM

The CCTA Risk Analysis and Management Method (CRAMM) was developed by the UK Central Computer and Telecommunications Agency (CCTA) in 1985.

The main objective of CRAMM was to provide a qualitative risk analysis and management tool for the security of IS. CRAMM is currently used in around 20 countries in trade and non-trade organisations due to its robust performance in securing IS against risks [118]. The method involves three stages: asset identification and valuation, threat and vulnerability assessment, and countermeasure selection and recommendation [86]. The following summarises these three stages [119]:

- Asset identification and valuation: in this stage, the assets of the organisation that support the business process are identified and valued.
- Threat and vulnerability assessment: in this stage, threats that might affect information system assets, and information system vulnerabilities, are identified. Risks are then analysed and assessed.
- Countermeasure selection and recommendation: in this stage, the countermeasures that are expected to mitigate the identified risks are proposed. This also includes improvements to the existing countermeasures.

3.2.4 Security Architecture and Engineering

This theme involves frameworks that suggest securing organisations' IS through secure enterprise architecture or processes and methods that can be used to evaluate how good the security engineering process of organisations is. The following are examples of standards and frameworks within this theme:

3.2.4.1 SABSA

The Sherwood Applied Business Security Architecture (SABSA) is an open-source framework for developing the risk-driven security architecture of enterprises. It is registered as a trademark of the SABSA limited organisation. The framework is a layered model, and it has been developed based on six vertical layers, as shown in Figure 3.6. Those layers are: Contextual Security Architecture, Conceptual Security Architecture, Logical Security Architecture,

Physical Security Architecture, Component Security Architecture, and Security Service Management Architecture [120-122].

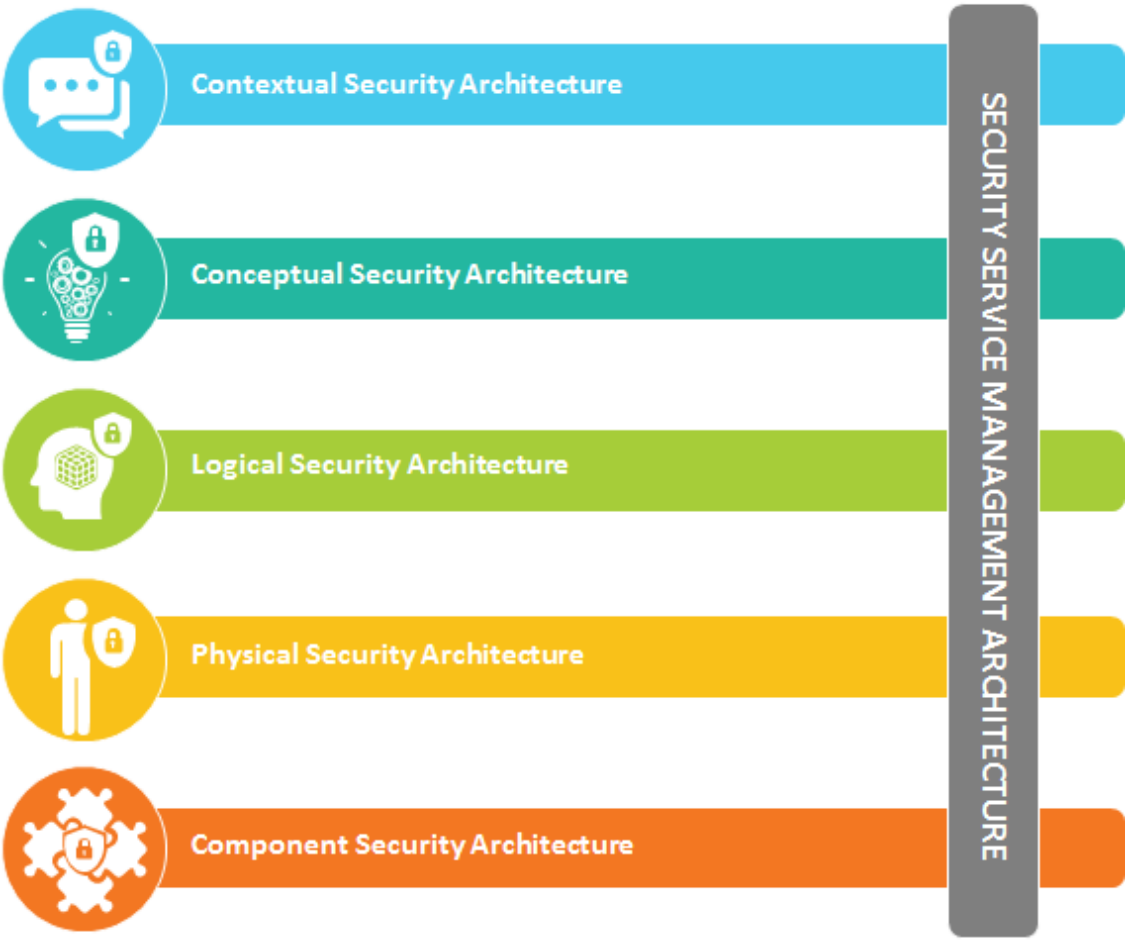

Figure 3.6: SBSA Layered Model [121]

The six vertical layers of the SABSA framework are integrated with six horizontal elements. The six elements are assets, motivation, process, people, location, and time. The vertical layers and horizontal elements provide 36 cells, which represent the framework matrix. Addressing the issues related to all 36 cells should cover the entire security architecture of enterprises [121-123].

The SABSA lifecycle consists of four phases as presented in Figure 3.7, which represent the entire development process of the enterprise security architecture. Those phases are: Strategy and Plans, Design, Implement, and Manage and

Measure. The Strategy and Plans phase embraces processes related to the first two layers' contextual and conceptual architectures, whereas the remaining layers are embraced in the Design phase. Processes that have been planned and designed are put into practice in the Implementation phase. The last phase is used to detect any performance deviation from what has been planned [124].

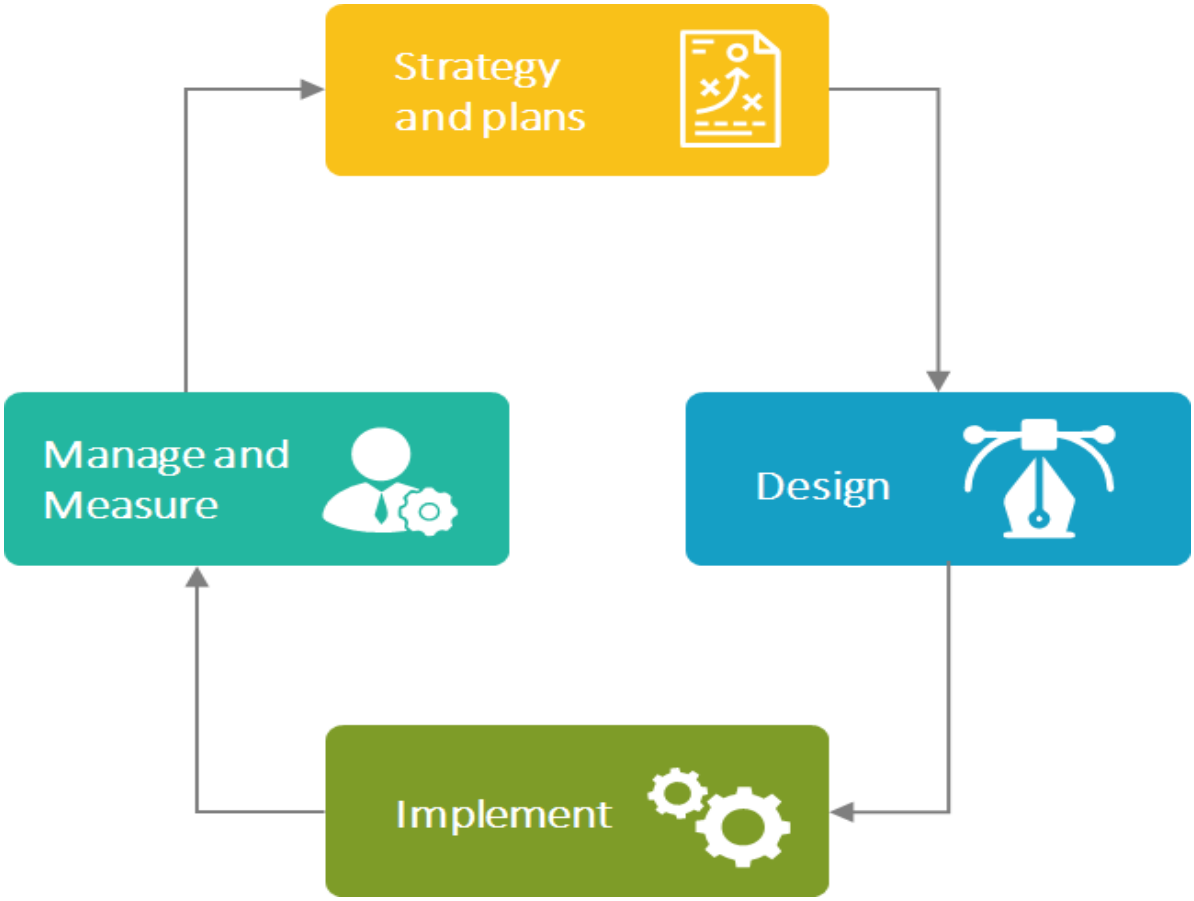

Figure 3.7: SABSA Lifecycle

3.2.4.2 SSE-CMM

The Systems Security Engineering - Capability Maturity Model (SSE-CMM), which became ISO/IEC 21827, is a process-model project that was originally sponsored by the National Security Agency (NSA). The SSE-CMM describes the essential features of the security engineering process that organisations must have to maintain an acceptable level of security engineering. To promote and advance the development of the model, the International Systems Security Engineering Association (ISSEA) was established. The model is based on two

categories, domain and capability. The domain category, which is called base practices, has 129 base practices grouped into 22 process areas, which are further grouped into three domains: security engineering, organisation, and project domains. The security engineering domain is categorised into three areas: risk, engineering, and assurance. The base practices represent the best practices required to ensure good security engineering processes. The capability category, which is called generic practices, has five Capability Levels. The generic practices represent activities that are not security-specific, but can be applied to different domains such as management and measurement. The generic practices should be performed as part of the base practices [13, 94, 125].

The SSE-CMM model can be seen as a tool for describing essential security activities that need to be achieved by organisations to maintain a good security engineering process. Additionally, the SSE-CMM model can be used to evaluate how good the security engineering process of organisations is [126].

3.2.5 ISMS Standards and Frameworks Summary

In Table 3.1, we provide a summary of the ISMS standards and frameworks [63-69, 71, 127-129] discussed in the previous sub-sections.

Table 3.1: ISMS Standards and Frameworks Summary

Approach	Main Focus	Strengths	Weaknesses
ISO/IEC 2700x series	Information security management	Comprehensive approach for information security management.	Low usability. Generality. Lack of adequate consideration of outsourced projects.
NIST SP 800 - series	Information security management	Comprehensive Approach for managing information security.	Low usability. Generality. Lack of adequate consideration of outsourced projects.
GMITS	Information security management	Provides a good foundation for managing information security.	Low usability. Lack of adequate consideration of outsourced projects.

Approach	Main Focus	Strengths	Weaknesses
COBIT	IT governance and service management	Holistic approach for IT governance. Can be integrated with other standards.	Lack of adequate consideration of outsourced projects. Low usability.
ITIL	IT governance and service management	Alignment with business needs. Service delivery efficiency.	Lack of adequate consideration of outsourced projects. Low usability.
OCTAVE	Risk management	Critical assets identification. Risks analysis focus. High usability.	Inadequate security requirements management. No compliance management. No consideration of outsourced projects.
CORAS	Risk management	Assets identification. Threat Scenarios. Incident Identification.	Inadequate security requirements management. No compliance management. No consideration of outsourced projects.
CRAMM	Risk management	Assets identification. Threat Identification. Security Controls Identification.	Inadequate security requirements management. No compliance management. No consideration of outsourced projects.
SABSA	Security architecture and engineering	Comprehensive approach for enterprise security architecture. Can be integrated with other standards.	Low usability. Lack of details of how to implement it. Lack of adequate consideration of outsourced projects.

Approach	Main Focus	Strengths	Weaknesses
SSE-CMM	Security architecture and engineering	Advanced security engineering as a defined, mature, and measurable discipline.	Low usability. More focused on system and software development. Lack of adequate consideration of outsourced projects.

3.3 ISMS Standards and Framework Evaluation

The outsourcing context differs from the conventional one. In the outsourcing context, environments are less stable and more systems are integrated together [130]. Therefore, it is more likely that existing ISMS standards and frameworks achieve different results to those they were intended to achieve. The outsourcing background given in the previous chapter (Section 2.7) showed the specific security needs that should be taken into account in order to effectively manage the security and compliance risks of outsourced IT projects. We will use these security needs to review the existing ISMS standards and frameworks to assess their applicability to managing outsourcing security risks effectively. Utilising the review outcome, we can decide whether we can customise one of them or whether we have to propose a new approach capable of managing the security risks of outsourcing effectively.

3.3.1 Evaluation Criteria

To explore the ability of existing ISMSs to manage the security and compliance risks of outsourced IT projects, we propose specific criteria based on the security needs that have been identified in Section 2.7. These criteria were drawn up based on the analysis of outsourcing business practices and the available literature provided in the previous chapter (specifically Sections 2.6 and 2.7). The proposed criteria are restated as follows:

- Security Requirements Management: the ISMS should be comprehensive. It should establish a complete methodology that is capable of managing security risks effectively. To do so, the ISMS should cover different security items. It should at least cover the following items:
    - Information Security Policy.
    - Communications and Operations Management.
    - Access Control.
    - IS Acquisition, Development, and Maintenance.
    - Asset Management.
    - Incident Management.
    - Business Continuity Management.
- Security Risks Management: security risks are not only technical. Therefore, any ISMS for managing the security risks of outsourced IT projects should manage security risks from different perspectives. ISMS should at least cover the following items:
    - Technical Risks.
    - Physical and Environmental Risks.
    - Human Resources Risks.
- Consideration of Outsourced IT Projects: to mitigate the security risks of outsourced IT projects, the ISMS should establish a method that takes into consideration the outsourcing context.
- Compliance management: The security programme should establish a method to enforce compliance properly.
- Usability: The ISMS should be usable for the outsourcing context from different perspectives. Outsourced projects usually last for a specific period of time. Therefore, the ISMS for managing the security risks of outsourced IT projects should be usable for this context. At least, the ISMS should be usable from the following perspectives:
    - Cost effectiveness.
    - Time efficiency.

- Simplicity and ease of use.

3.3.2 Evaluation Results

Having provided an overview for each ISMS standard and framework and identified the evaluation criteria, we have evaluated the existing ISMS standards and frameworks. The evaluation results are based on our own assessment and previous studies available in the literature [63-69, 71, 127-129]. In Table 3.2, we present the evaluation results.

In Table 3.2, there are three options, which represent the result of each criterion or factor:

- (√) when the criterion or factor is supported by the framework or standard.
- (≈) when the criterion or factor is partially supported by the framework or standard.
- (×) when the criterion or factor is not supported by the framework or standard.

Table 3.2: ISMS Standards and Frameworks Evaluation Results

Criteria	***ISO/IEC 2700x series***	***NIST SP 800 - series***	***GMITS***	***COBIT***	***ITIL***	***OCTAVE***	***CORAS***	***CRAMM***	***SABSA***	***SSE-CMM***
1-Security Requirements Management:										
Information Security Policy	√	√	√	√	√	×	×	×	√	√
Communications and Operations Management	√	√	√	√	×	≈	×	×	√	√
Access Control	√	√	≈	√	√	×	×	×	√	√
Information Systems Acquisition, Development, and Maintenance	√	√	√	√	×	×	×	×	√	√

Criteria	*ISO/IEC 2700x series*	*NIST SP 800 - series*	*GMITS*	*COBIT*	*ITIL*	*OCTAVE*	*CORAS*	*CRAMM*	*SABSA*	*SSE-CMM*
Asset Management	√	√	≈	√	√	√	√	√	√	√
Incident Management	√	√	√	√	√	×	×	×	≈	≈
Business Continuity Management	√	√	√	√	√	×	×	×	√	≈
2- Risks Management:										
Physical and Environmental Risks	√	√	√	≈	×	≈	≈	≈	√	√
Human Resources Risks	√	√	√	≈	×	≈	≈	≈	√	√
Technical Risks	√	√	√	≈	≈	√	√	√	√	√
3- Consideration of outsourced projects:	≈	≈	≈	×	×	×	×	×	≈	×
4- Compliance	√	√	√	√	√	×	×	×	√	√
5- Usability:										
Cost effectiveness	×	×	×	×	×	√	√	√	×	×
Time efficiency	×	×	×	×	×	√	≈	√	×	×
Simplicity and easiness	×	×	×	×	×	√	√	√	×	×

3.3.3 Evaluation Analysis

As can be seen from Table 3.3, the ISO/IEC 2700x and NIST SP 800 series met 73% of the evaluation criteria. However, 80% of the organisations around the world use the ISO/IEC 2700x series for the monitoring, review, maintenance and improvement of their information security management systems [71]. The wider concept and scope provided by the ISO/IEC 2700x series make them more applicable to all organisations for internal information security management, regardless of their shapes and sizes [68].

Although ISO/IEC 2700x and the NIST SP 800 series play a very important role in managing internal information security management, they suffer from low usability (cost effectiveness, time efficiency, simplicity and ease of use) in the

outsourcing context. In order to implement them effectively, the organisation would need access to a large bank of resources. When outsourcing, budget constraints and adherence to the project schedule are important; therefore ease of use, cost effectiveness, simplicity and time efficiency are paramount [67].

Table 3.3: Criteria Summary

	ISO/IEC 2700x series	***NIST SP 800 - series***	***GMITS***	***COBIT***	***ITIL***	***OCTAVE***	***CORAS***	***CRAMM***	***SABSA***	***SSE-CMM***
Count										
√	*11*	*11*	*9*	*8*	*6*	*5*	*4*	*5*	*10*	*9*
≈	*1*	*1*	*3*	*3*	*1*	*3*	*3*	*2*	*2*	*2*
×	*3*	*3*	*3*	*4*	*8*	*7*	*8*	*8*	*3*	*4*
Percentage										
√	73%	73%	60%	53%	40%	33%	27%	33%	67%	60%
≈	7%	7%	20%	20%	7%	20%	20%	13%	13%	13%
×	20%	20%	20%	27%	53%	47%	53%	53%	20%	27%

Based on the results in Section 3.3.2, the main weaknesses of ISMS standards and frameworks are summarised as follows:

- Lack of or weak comprehensive security methodology: most of the reviewed ISMSs suffer from a lack of comprehensive security methodology. Only general recommendations are provided without a clear explanation of how to apply them.

- Lack of adequate consideration of compliance: ISMSs suffer from the lack of a robust method for compliance enforcement. The majority of them provide only general recommendations for compliance without any explanation of how to enforce compliance.
- Usability: most of the ISMSs reviewed in this chapter, except the risk management standards and frameworks, suffer from low usability as their correct implementation requires large amounts of resources [67]. In our criteria, the usability criterion consists of three factors: cost effectiveness, time efficiency, and simplicity and ease of use.

- Cost effectiveness: the reviewed ISMSs require a large budget for a security programme to be established within an organisation. For many organisations, especially organisations with senior managers who do not adequately realise the importance of information security, the required budget is high and difficult to justify.
- Time efficiency: the time required to complete the implementation of the reviewed ISMSs is relatively long. The ISMSs require different aspects to be covered, such as those related to people, and technical and physical aspects. Implementing the processes and procedures proposed by the ISMSs to mitigate the risks associated with these aspects might in many cases exceed the time required for the execution of outsourced IT projects.
- Simplicity and ease of use: the reviewed ISMSs require professional knowledge and skills to plan, develop, and maintain them. With a lack of detailed guidelines that explain how to implement ISMSs, in many cases organisations are left without the knowledge or skills necessary to implement the ISMSs effectively.

In the context of outsourced projects, the ISMS needs to be clear and easy, inexpensive, and it should be possible to implement it in a short period of time. Otherwise, the project schedule and budget might be seriously affected.

- Generality: the reviewed ISMSs in general represent general best practices and recommendations that can be used to mitigate the security risks associated with information systems. Nevertheless, security requirements differ from one organisation to another. This variation in security requirements is not addressed properly by these ISMSs [13]. This does not mean that there is a complete failure to address the different security requirements of organisations, but it

means that what might be neglected by one ISMS is covered by another and vice versa, according to the main focus of each ISMS.

- Lack of adequate consideration of outsourced projects: ISMSs are mainly designed to deal with the internal processes of organisations. They are not designed to deal with the security risks of outsourced IT projects [14]. Such risks are rarely addressed, and if they are, they are no more than general requirements without detailed guidelines that explain how to comply exactly with these requirements.

Based on the results provided in Section 3.3.2, the following points can be extracted:

- There is no single framework or standard that satisfies all the security and compliance needs for managing the security and compliance risks of outsourced IT projects.
- All reviewed standards and frameworks are not designed specifically for managing the security and compliance risks of outsourced IT projects. Therefore, updating these standards and frameworks to fit the outsourced IT projects context makes them more complicated, thus consuming more time and resources.
- The reviewed standards and frameworks differ in their strengths and weaknesses. For instance, risk management standards and frameworks provide high usability but low security requirements management, whereas the standards and frameworks of information security management provide high security requirements management but low usability. Therefore, any proposed solution should benefit from the strengths of existing ISMS standards and frameworks and provide some solutions that could overcome their weaknesses.
- The usability criterion has the lowest support from all standards and frameworks, with the exception of the risk management standards and frameworks.

As a conclusion, the reviewed ISMS standards and frameworks have contributed to improving information security management in general. However, it can be seen from the evaluation results that the security and compliance management of outsourced IT projects have still not been studied in depth. This gap needs to be investigated and studied in order to resolve it. To manage the security risks of outsourcing effectively, several elements need to be taken into consideration, such as establishing a comprehensive methodology for managing security requirements, managing security risks from different perspectives, managing compliance, and being usable from different perspectives (e.g. cost effectiveness, time efficiency and simplicity).

3.4 Summary

In this chapter, existing ISMS standards and frameworks have been categorised into four themes: Information Security Management, IT Governance and Service Management, Risk Management, and Security Architecture and Engineering. For each theme, representative examples of leading ISMS standards and frameworks have been provided. Their ability to effectively manage the security and compliance risks of outsourced IT projects was assessed based on specific criteria identified for this purpose. These criteria involve security requirements management, risk management, the consideration of outsourced projects, compliance and usability.

Despite the enormous benefit of ISMSs with regard to achieving information system confidentiality, integrity, and availability, and mitigating security risks, they still do not satisfy the security and compliance needs of outsourced IT projects. Most of the reviewed ISMSs do not take into consideration the outsourcing context. In the outsourcing context, where environments are less stable and more systems are integrated together, ISMSs should be comprehensive. They should establish a complete methodology that is capable of managing the security and compliance risks of outsourced IT projects effectively. The ISMS should manage a range of security risks, such as technical, human resources, physical and environmental risks. As outsourced IT projects usually

last for a specific period of time, the ISMS should take this into consideration and be usable for the outsourcing context in terms of cost effectiveness, time efficiency, and simplicity and ease of use. The reviewed ISMSs have many weaknesses such as low usability and generality, and the lack of adequate consideration of the security risks associated with outsourced IT projects.

In the following chapter, and based on the Chapter 2 and 3 outcomes, the requirements for effectively managing the security and compliance risks of outsourced IT projects will be identified.

Chapter 4 Requirements for Managing the Security and Compliance Risks of Outsourced IT Projects

The previous chapter reviewed existing ISMS standards and frameworks. Their strengths and weaknesses in managing the security and compliance risks of outsourced IT projects were identified. The gap in the literature and the need for a new approach that could tackle the weaknesses of existing frameworks were also discussed in the previous chapter. In this chapter, the requirements for effectively managing the security and compliance risks of outsourced IT projects will be determined.

4.1 Introduction

Before we proceed to developing a solution for managing the security and compliance risks of outsourced IT projects, we need to identify the requirements that the proposed solution should fulfil. The following sub-sections discuss these requirements.

The rest of this chapter is structured as follows: we identify the security and compliance requirements in Section 4.2. The case study of outsourced IT projects is presented in Section 4.3. We finally summarise this chapter in Section 4.4.

4.2 Security and Compliance Requirements

In order to design a solution that satisfies the security and compliance needs of outsourced IT projects, it is important to firstly specify the requirements that need to be considered when developing the proposed solution. The following requirements were proposed after reviewing existing ISMS standards and frameworks and identifying their weaknesses, in addition to analysing the literature in the previous chapters.

The requirements take into account the importance of aligning the security management of outsourcing with project management, as well as considering factors that contribute to building secure and protected environments. Security

risks in the outsourcing context are taken into consideration from different perspectives. Compliance enforcement, usability, flexibility and reusability are taken into consideration as well.

4.2.1 Aligning Security Management with Project Management

Modern project management emerged and became a discipline in the late 1950s and at the beginning of the 1960s [131]. Since then, different project management standards have been developed and practised across different industry domains [132]. The uncertainty associated with project failures has increased the adoption of project standards among different types of organisations [133]. Project management standards provide structured methods for managing projects with the aim of completing projects successfully, which achieves organisations' objectives. Such standards can be applied to any type of project, regardless of their cost, time, or any other constraints [132].

Today, there are several leading standards and frameworks for project management that can be used. These standards and frameworks are available for project managers who are responsible for delivering projects to their customers according to their requirements [134]. Although project management standards and frameworks do not guarantee any success, they provide general best practices that can be tailored to suit projects in order to improve the planning and controlling of such projects. Several project standards, such as the Project Management Body of Knowledge (PMBOK), provide educational and training programmes that confer certifications [135].

Aligning security management with project management could provide several benefits. Project phases could help with allowing separate security risk management. The rationale behind this separation is that it allows security requirements to be identified and broken down based on the project phases, instead of setting security requirements for the whole project. This will allow the project team to identify security requirements more easily and they can then

concentrate on activities that belong to each particular phase. Other resources can be utilised in other project activities.

The separation could also help with achieving security requirements on time. Each project phase has its own security activities. Such separation provides a better understanding of security requirements. If project resources are allocated efficiently, the project's execution time will not be affected.

The following sub-sections provide an overview of three of the leading project management standards [135, 136]. Those standards are Project Management Body of Knowledge (PMBOK), Projects In Controlled Environments (PRINCE2), and International Competence Baseline (ICB).

4.2.1.1 PMBOK

The PMBOK standard has been developed by a US non-profit organisation called the Project Management Institute (PMI). The first white paper of PMBOK was published in 1987. This standard provides best practices related to processes, techniques, and tools that can be used to enhance a project's success. It can be applied to any type of project across different industry types. The PMI is widely recognised worldwide, with more than half a million members and a continuous annual growth in more than 180 countries [135, 137].

The PMBOK standard provides guidance for project management in five process groups[132]. The process groups are: Initiating, Planning, Executing, Monitoring and Controlling, and Closing. In the process groups, there are 47 processes, divided into ten knowledge areas:

- Integration Management
- Scope Management
- Time Management
- Cost Management
- Quality Management
- Human Resource Management

- Communications Management
- Risk Management
- Procurement Management
- Stakeholder Management

4.2.1.2 PRINCE2

The Projects In Controlled Environments (PRINCE2) is a project management standard that has been developed by a UK agency called the Office of Government Commerce (OGC). It was first published in 1996 [135]. PRINCE2 was derived originally from a previous method called PROMPTII, which was used to develop PRINCE in 1989 [133]. The standard is a process-based method developed to be used as a de facto standard for IT projects across government agencies in the UK. Since then, the standard has been recognised internationally, especially in Europe and Australia. It has been adopted by different agencies in public and private domains [138].

PRINCE2 provides guidance on how to manage projects successfully by using seven principles, seven themes, and seven processes. The seven principles are business justification, lessons learned, defining roles and responsibilities, managing by phases, managing by exception, being product focused, and tailored to fit the project environment. The seven themes are business case, organisation, quality, plans, risks, changes and progress. The seven processes, which have 40 activities, are starting a project, initiating a project, directing a project, controlling a stage, managing stage boundaries, managing product delivery and closing a project [135, 139].

4.2.1.3 ICB

The International Competence Baseline (ICB) standard was developed by a non-profit international organisation called International Project Management Association (IPMA). The IPMA is one of the oldest project management organisations, and it has a strong presence in European countries. The first version of the ICB standard was made public in 1998. The ICB standard forms the

fundamental knowledges required for project personnel who are seeking to achieve the four-level ICB certifications. These certifications represent a career path in project management, from entry level (level D) to the highest level (level A) [135, 140, 141].

The ICB standard divides project management into 46 elements of competences. Those 46 elements are clustered into three groups: technical (20 elements), behavioural (15 elements), and contextual competences (11 elements). For each of the three competence groups, ICB provides an introduction, process stages, topics, certification grades and other competences related to the current competences. The ICB applies the 46-competence elements to the project manager and project teams in order to improve the project success rate. It focuses on project personnel skills and capabilities [135, 142].

4.2.1.4 Analysis

The processes of PRINCE2 are similar and comparable to the PMBOK process groups. Although the number of processes is different (40 in PRINCE2 and 47 in PMBOK), the major activities are covered in both standards. Also, the PRINCE2 themes and the PMBOK knowledge areas are similar, with the exception of procurement in PMBOK, which is not covered in PRINCE2. While PRINCE2 focuses on key risks to improve the project success rate, PEBOK focuses on applying processes, techniques and tools. Projects are driven by business cases in PRINCE2 while projects are driven by stakeholders' requirements in PMBOK [135, 140].

For the ICB standard, the differences are more obvious. ICB focuses on project personnel skills and capabilities to improve the project success rate. In contrast, PMBOK concentrates on project processes and techniques that might be employed by project managers and teams. Behavioural competences (personal relationships) are emphasised in ICB whereas technical skills are emphasised in PMBOK. Both skills are important in projects and it is critical to balance them in

order to improve the project success rate [135]. Table 4.1 presents the key characteristics of these three standards.

Table 4.1: Standards' Characteristics

	PMBOK	PRINCE2	ICB
Standard Type	Process-focused guidance	Product-focused methodology	Competence-focused guidance
Method	10 Knowledge areas (47 processes)	7 Principles, 7 Themes, 7 Processes (40 activities)	46 Competences
Focus	Processes and technical skills focus. More comprehensive approach. Project requirements emphasis.	Project key risks focus. Project control enhancement. Business case use.	Capability and skill assessment focus. Behavioural competences emphasis. Satisfaction and quality prominence.

Although different project management standards are available, PMBOK is considered internationally as a de facto standard for managing projects [140]. The standard provides a more comprehensive approach than the other project management standards. It is preferred with outsourced IT projects, which require large teams for project implementation, engagement with different stakeholders, and high commitment for clients [132]. The following summarises the benefits of PMBOK compared to the other standards [135, 140, 143]:

- Knowledge-based approach with comprehensive coverage of a wide range of project practices.
- Forms the base for most other project management standards.
- Easy and learnable knowledge areas.
- Can be applied to all project types and sizes.
- Stronger approach for the integration of project processes.
- Stronger approach for project communication management.

4.2.2 Managing Security Requirements

To manage the security requirements of outsourced IT projects effectively, the security programme or framework should establish a complete and clear

methodology that is capable of managing the security of outsourced IT projects adequately. It should consider all of the factors that contribute to achieving a comprehensive security programme or framework. To do so, the following items at least should be included in such a programme:

- Information Security Policy.
- Communications and Operations Management.
- Access Control.
- Information Systems Acquisition, Development, and Maintenance.
- Asset Management.
- Incident Management.
- Business Continuity Management.

4.2.3 Managing Security Risks

The security risks of outsourced IT projects are not only technical. Therefore, any security programme or framework for managing the security risks of outsourced IT projects should manage risks from different perspectives. The programme or framework should cover at least the following items:

- Technical Risks.
- Physical and Environmental Risks.
- Human Resources Risks.

Threat classification plays a vital role in managing the security risks of outsourced IT projects. It is used to identify potential security threats to the project assets at early stages of the project's execution. Threat classification is not a brainstorming process that the project teams can use to investigate security threats. Such a brainstorming may miss large threat possibilities, which might be exploited by attackers. Attackers may need only one security weakness to break the entire system. Threat classification should follow a systematic approach to capture the potential threats that the project might face [144].

In the literature, researchers from diverse domains have investigated threat classification. Different approaches for classifying threats have been proposed. National and international organisations such as ISO and NIST have also proposed other threat classification taxonomies. The literature review has shown several attempts at classifying the threats that face information systems. Those threat classification approaches can be classified into two main categories: approaches based on attack techniques, and approaches based on attack impacts [145].

- Threat classification approaches based on attack techniques: in this type of threat classification, techniques that are used by attackers to exploit any system vulnerabilities are used to classify information system threats. The following represent examples of this classification.
    - The three dimensional model: in this approach, the threats are classified using three factors: agent, motivation and localisation. The agent factor is a threat actor that imposes a security risk on an information system. It is classified into human, technological or majeure. The motivation factor is either deliberate or accidental threats, which represent the cause for committing this action. The localisation factor represents the threat source, which can be classified as either an internal or external threat [145].
    - The threat cube model: this model uses three criteria for classifying information system threats: threat frequency, threat area and threat source. The threat frequency represents how often the threat takes place. The threat area focuses on which part of the system will be exploited by the threat. The threat source is categorised into two types: insiders and outsiders [145, 146].
    - The threat pyramid model: this threat classification technique is used to model deliberate threats using three factors: prior knowledge that attackers possess about the system, area

criticality and loss. The first factor represents how much knowledge attackers may have about areas such as system design and system infrastructure. The second factor represents the criticality of the part of the system being exploited by the attacker. The third factor represents the potential losses that will be experienced if the threat occurs [145, 147].

- Threat classification approaches based on attack impact: in this type of threat classification approach, the goals of attackers are used to classify threats. The following are examples of these approaches.
    - Microsoft STRIDE model: this approach classifies threat impact into six categories: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. The first letter of each category is used to form the STRIDE acronym [148, 149].
    - ISO 7498-2 model: in this threat classification approach, the threat impact is classified into five categories: information or resource destruction, information corruption or modification, information or resource theft, removal or loss, information disclosure, and service interruption [145].

Although many threat classification approaches have contributed to identifying information system threats more accurately, they still suffer from some limitations. The main limitation is that most of these approaches use only two or three criteria for classifying system threats. This limitation affects the approaches' ability to provide a comprehensive classification that is capable of identifying potential security threats. As a result, they are not exhaustive and do not provide a comprehensive list of potential security threats. Such approaches might be beneficial in stable environments such as small businesses where threats are relatively low and stable [145, 146].

In order to manage the security threats of outsourced IT projects properly, the threat classification approach needs to be comprehensive and take into

consideration the context of outsourcing. Threats in this context are imposed by different parties such as providers, the client, and so on. Therefore, security threats need to be managed from different perspectives, which suit the outsourcing context. Moreover, the threat classification approach needs to achieve some desired properties to provide a comprehensive threat classification. Those properties are described briefly as follows [145, 150, 151]:

- Mutually exclusive: every threat should fit into only one category and there is no overlapping between categories.
- Collectively exhaustive: every category should include all possible potential threats.
- Unambiguous criteria: categories are clear and there are specific criteria to identify each category of threat.
- Repeatable: the result of threat classification for the same application is generally the same, regardless of who carries out the threat classification.
- Comprehensible and useful: provides comprehensive results and is useful not only for security experts, but also for users with no deep security background.

Following threat identification, the security risks associated with these threats need to be estimated. Different risk estimation techniques (e.g. qualitative, quantitative, semi-quantitative) can be used to estimate the likelihood and magnitude of the security risks that affect confidentiality, integrity and availability.

- Qualitative techniques: are subjective and based on security experts' judgements and perceptions as they carry out the risk assessment processes. The results are usually expressed in qualitative categories such as high, medium, or low. Scenarios and questionnaires might be used to estimate risk categories. Qualitative techniques do not require a deep mathematical background, which make them easier and simpler than other methods [18].

- Quantitative techniques: use different mathematical methods such as Bayesian networks and fuzzy logic to express risk values based on numbers. Although these techniques might provide more accurate results of risk assessment, especially when they are carried out by experts, they consume much more time than qualitative techniques and are more difficult to understand for non-experts [18]. Figure 4.1 gives some advantages and disadvantages of qualitative and quantitative techniques.

Quantitative methods	*Qualitative methods*
ADVANTAGES	
Applicability to all assets	Simple risk calculation
Mathematical foundation	Usefulness when asset value is irrelevant or unknowable
Using a management specific language (Support cost benefit decision)	Less time consuming
Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.	Easier to involve people who are not experts on security or computers.
DISADVANTAGES	
Inappropriateness of monetary asset value	Coarse granularity
Inappropriateness of general statistics	Inability of cost benefit decision
Time consuming, requires much preliminary work	Subjective results, depend on quality of risk management team

Figure 4.1: Qualitative and quantitative techniques' advantages and disadvantages [18]

- Semi-quantitative techniques: express risk assessment results using a combination of number ranges such as 1-25, 26-75 and 76-100 and categories such as low, medium and high. Such techniques combine qualitative and quantitative advantages. For instance, when the risk is assessed as 80, the number can be easily interpreted against a level category (high), which can be understood easily by non-experts such as decision makers [19].

Having identified security threats and estimated their impact on confidentiality, integrity and the availability of project assets, countermeasures (controls) that mitigate security risks need to be proposed and implemented. To manage the implementation of security countermeasures accurately, roles and responsibilities need to be determined clearly. Various methods exist for managing human resource roles and responsibilities. The majority of these methods fall into three categories: the hierarchical method, matrix method and text-oriented method [152].

- Hierarchy-based method: in this method, the structure of organisations (top-down format) is used to show high-level areas of roles and responsibilities, and the relationships between the organisation departments, units and teams. Figure 4.2 shows a representative example of hierarchy-based methods.

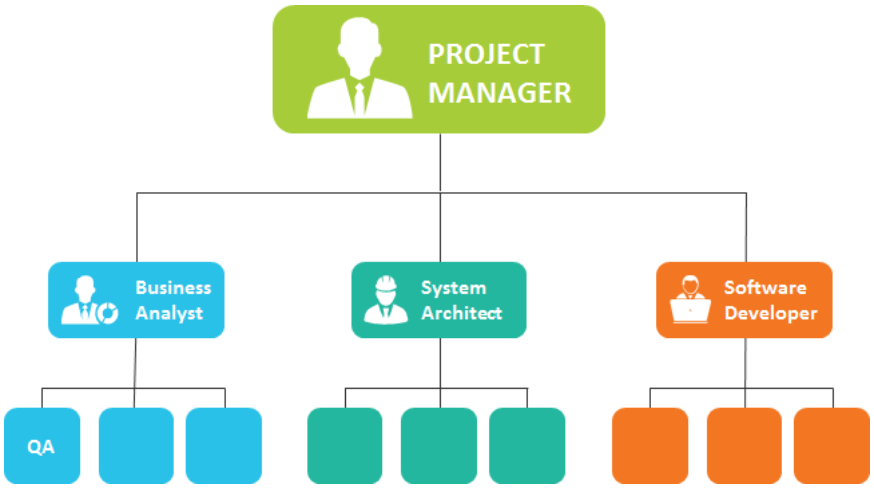

Figure 4.2: Hierarchy-based method [152]

- Matrix-based method: in this method, activities are assigned to team members using the Responsibility Assignment Matrix (RAM). Responsible, Accountable, Consult and Inform (RACI) represents an example of RAM, as shown in Figure 4.3. If a person is responsible for a task, he has to carry out the task. If the person is accountable for the task, he is answerable for the task or any decisions related to it. Only one person can be assigned to the task with the role "Accountable". The "Consult" role is assigned to the person who will be consulted prior to a decision or action for a given task, whereas the person who needs to be informed after completing the task or taking a decision related to it takes the role "Inform" [153].

RACI CHART	PERSON				
Activity	Ann	Ben	Carlos	Dina	Ed
Define	A	R	I	I	I
Design	I	A	R	c	c
Develop	I	A	R	c	c
Test	A	I	I	R	I

Figure 4.3: Matrix-based method [152]

- Text-oriented method: in this method, the responsibilities of team members are detailed using a text format, as shown in Figure 4.4.

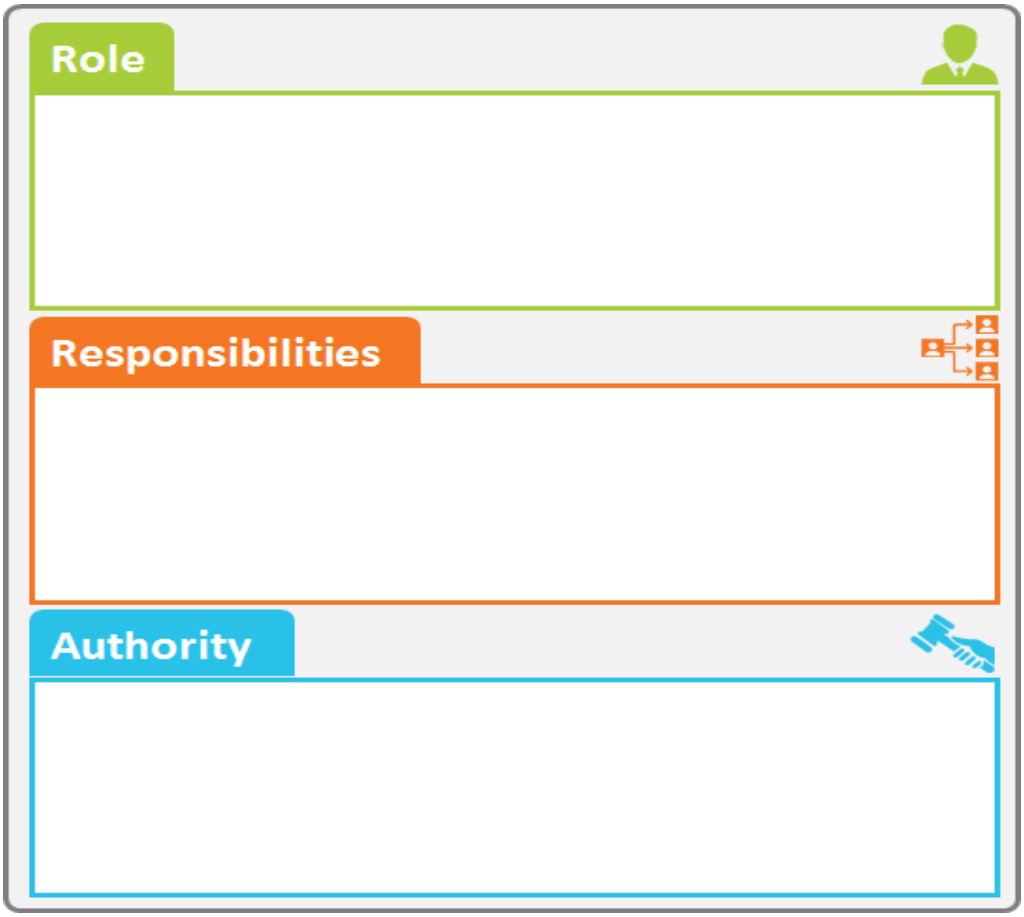

Figure 4.4: Text-oriented method [152]

4.2.4 Managing Compliance

The security programme or framework should establish a method to enforce compliance properly. Ensuring compliance with security requirements is an essential part of information systems security, as unenforced security requirements will not achieve the expected security goals [59]. Compliance management should at least take into consideration the following items:

- Compliance with security requirements.
- Compliance with laws, regulations, contracts, SLAs, etc.

4.2.5 Enhancing Flexibility

In the outsourcing context, where environments are less stable and more systems are integrated together, it is more likely that the planned security

solutions will change over the project's phases, in order to meet new security requirements or to provide more efficient methods for dealing with the current security requirements. The security programme or framework should therefore embrace a flexibility feature to accommodate any need for change or improvement. The Plan-Do-Check-Act (PDCA) model [154] is an example that can be used to continuously improve security solutions during the project phases.

4.2.6 Improving Usability

Outsourced projects usually last for a specific period of time. Therefore, any security programme or framework for managing the security of outsourced IT projects should be usable for this context from different perspectives. At least, the programme or framework should be usable from the following perspectives:

- Cost effectiveness.
- Time efficiency.
- Simplicity and ease of use.

4.2.7 Enhancing Reusability

Outsourced IT projects may have different things in common such as environments, assets, etc. Therefore, any security programme or framework to be used for managing the security of outsourced IT projects should utilise previous threat identification and risk assessment for new outsourced IT projects. This will speed up the process and provide a more efficient way to allocate resources (these can be allocated to other tasks instead of repeating previous tasks). The framework should also be independent from different constraints such as the project type, cost, or size, in order to provide a general methodology that can be tailored to fit any project. It is essential that the security programme or framework is developed to fit different project types, sizes or missions.

4.3 IT Outsourcing Case Study

This case study represents a simplified but real outsourced IT project. It was used to assess the applicability of the existing ISMS standards and frameworks, which were discussed in Chapter 3, to managing the security and compliance risks of outsourced IT projects. It will also be used in Chapter 5 when developing the new framework, which will be used for managing security and compliance risks in the outsourcing context.

In the case study, a Middle-East country wishes, through its technical agent (we call this the client), to contract with a single preferred provider for designing, developing, and implementing a system that will collect and process Advanced Passenger Information (API) and Passenger Name Records (PNR). All airlines flying to, out or within the country must provide the client with the booking information (PNR) and the check-in data (API) of all passengers.

The API/PNR system will interface with airlines' Reservation Control Systems (RCS) to collect PNR data, and with airlines' Departure Control Systems (DCS) to collect the API data of all the passengers (inbound, outbound, transit or domestic). Small airlines (also buses and ships for land and sea borders) that do not have RCS or DCS will be able to provide their passengers' data over the Internet using the client's website.

The API/PNR system will be integrated with the client's existing critical applications, opened to the Internet, and executed on-site with the ability of the provider's staff to access different client data centres. The client's assets, including its watch list data and the API/PNR assets, must be protected from internal and external threats in order to achieve confidentiality, integrity and availability of the client information system, as well as the APP/PNR data and information provided. The question is how to effectively manage the security and compliance risks of the API/PNR system? The API/PNR system is large and complex as it will be integrated with the client's and stakeholders' systems. It also has a tight schedule and must be executed within 18 months. With the

existing ISMS standards and frameworks, the following issues will be encountered:

- Lack of a comprehensive methodology that tells project teams how to manage the security risks that might take place while implementing the project. With the lack of such a methodology, project teams will have to spend a great deal of time finding suitable security recommendations that are applicable to the API/PNR project.
- Absence or weak methods for enforcing compliance with security requirements and controls. Clients in many cases are left with an inability to enforce compliance properly. If they want to audit compliance, they might have to hire external auditors, which will add extra costs and time.
- Flexibility and usability difficulties. In outsourcing projects, it is expected that security requirements change over time due to new risks or environment changes. Without a clear method to implement changes, these changes might introduce new risks. These difficulties can also lead to delays in the project schedule and increase costs, as resources will be needed to analyse and plan the new changes.
- Weak threat classification approaches. In the outsourcing context, threats arise from different agents such as providers, clients, external attackers, and environmental and physical threats. Therefore, the threat classification approach used should be systematic and comprehensive. It should also consider risks from different perspectives to be able to identify the potential security threats that the project might face.

In the above case study, existing ISMS standards and framework are not able to effectively manage the security and compliance risks of outsourced IT projects. In Chapter 5, we will use this case study to illustrate how the OSCR framework overcomes these issues.

4.4 Summary

In this chapter, the requirements for managing the security and compliance risks of outsourced IT projects have been identified. To design an effective solution, the security programme or framework should meet specific requirements such as aligning security management with project management, establishing a comprehensive methodology for managing security requirements, managing security risks from different perspectives, managing compliance, enhancing flexibility and reusability, and improving usability.

The case study presented in this chapter shows that different security and compliance risk issues exist when using existing ISMSs. The Lack of a comprehensive methodology, improper compliance enforcement, and weak threat classification approaches are examples of these issues.

In the next chapter, a framework will be designed for managing the security and compliance risks of outsourced IT projects. It will be designed to meet these requirements and to be able to manage the variation of security requirements, as well as to provide a methodology that guides organisations for the purpose of security management and implementation.

Chapter 5 Management of Outsourced IT Project Security and Compliance Risks

The previous chapter proposed specific requirements for effectively managing the security and compliance risks of outsourced IT projects. These requirements provide a broad and comprehensive base for developing any solution to be used in an outsourcing context. In this chapter, we present our framework, which is designed to meet the proposed requirements.

5.1 Introduction

Although the framework that will be introduced in this chapter for managing the security and compliance risks of outsourced IT projects is independent from any project management standard or framework, the five process groups (project phases) of the Project Management Body of Knowledge Standard (PMBOK) will be utilised. PMBOK is considered internationally as a de facto standard for managing projects [155], and it is expected that the majority of providers use this standard. For these reasons, we have built our framework on the project phases of the PMBOK standard. Nevertheless, the framework can work with or without any project management standard. Its own activities are identified and independent from any standard.

The rest of this chapter is structured as follows: we introduce the framework to be used for managing the security and compliance risks of outsourced IT projects in Section 5.2. We discuss the framework features in Section 5.3, and we summarise this chapter in Section 5.4.

5.2 Managing the Security and Compliance Risks of Outsourced IT Projects

In this section, we propose a framework for managing the security and compliance risks of outsourced IT projects, called the OSCR framework (Outsourcing Security and Compliance Risks framework). The OSCR framework

utilises project phases (initiating, planning, execution, monitoring and controlling, and closing) and the Plan-Do-Check-Act (PDCA) model. Each project phase has its own security activities. During the planning, execution, and monitoring and controlling phases, the PDCA model is applied. Managing project security and compliance risks should be aligned with the project phases as discussed in the previous chapter, with the consideration of improvements during the project's execution to improve flexibility. Figure 5.1 presents the main architecture of the OSCR framework, while Table 5.1 provides a summary of the phases, main units, deliverables and responsibilities of the OSCR framework. The workflow of the OSCR framework is presented in Figure 5.2.

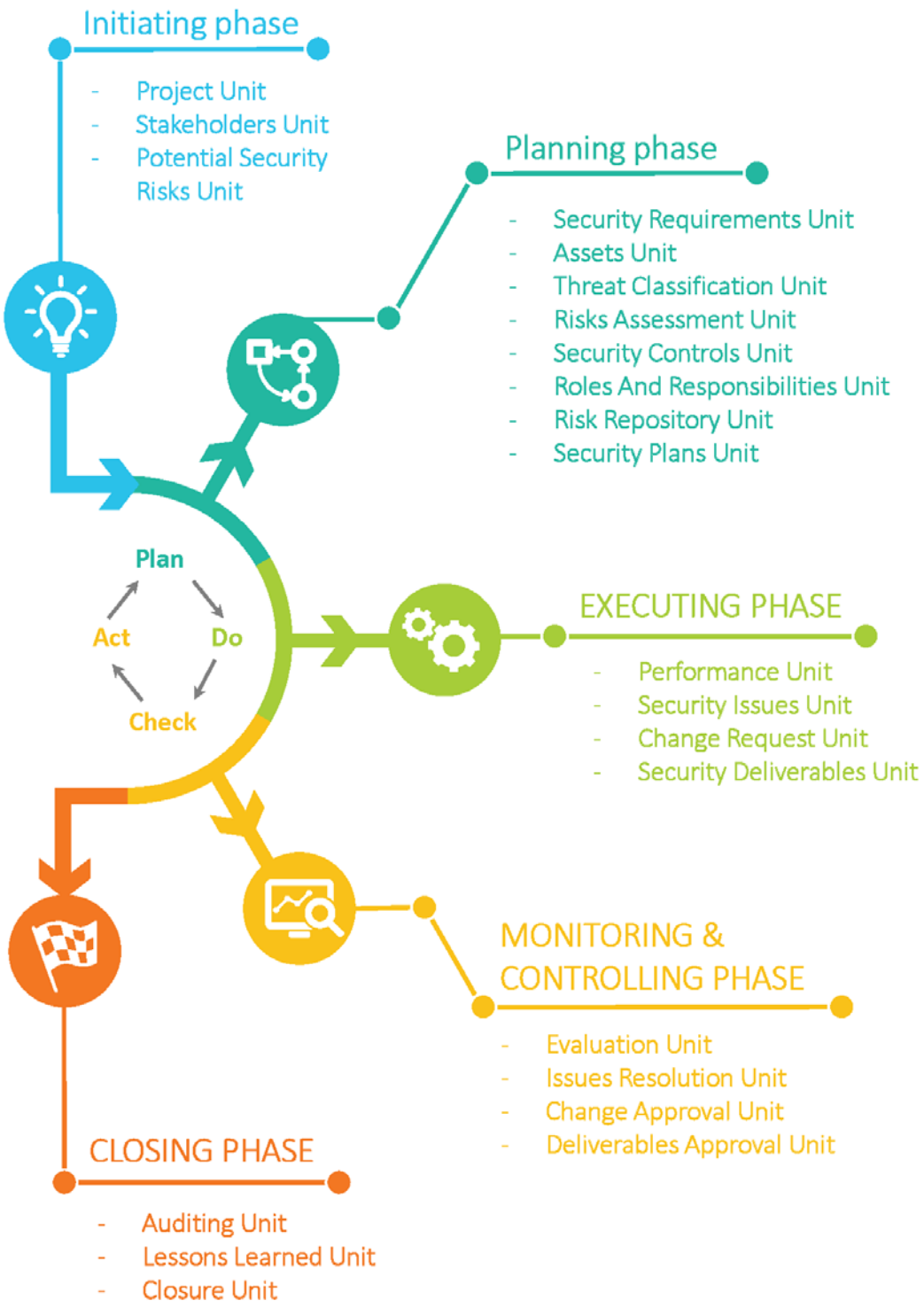

Figure 5.1: OSCR Framework

Table 5.1 : OSCR Framework's Units, Deliverables and Responsibilities

	Main Units	**Main Deliverables**	**Responsibility**
Initiating Phase	Project Unit	Project data identification	The Client
	Stakeholders' Unit	Project stakeholders' data	
	Potential Security Risks Unit	Potential security risks list	
Planning Phase	Security Requirements Unit	Security requirements list	The Client & Provider
	Assets Unit	Assets list	
	Threat Classification Unit	Threats list	
	Risk Assessment Unit	Risks exposure and prioritisation	
	Security Controls Unit	Security controls list	
	Roles And Responsibilities Unit	Roles and responsibilities details	
	Risk Repository Unit	Risks document	
	Security Plans Unit	Security plans	
Executing Phase	Performance Unit	Performance reports	The Client & Provider
	Security Issues Unit	Security issues reports	
	Change Request Unit	Change requests	
	Security Deliverables Unit	Security deliverables	
Monitoring and Controlling Phase	Evaluation Unit	Performance improvements	The Client & Provider
	Issues Resolution Unit	Issues resolution	
	Change Approval Unit	Changes approval	
	Deliverables Approval Unit	Deliverables approval	
		Project plans and document updates	
Closing Phase	Auditing Unit	Auditing report	The Client & Provider
	Lessons Learned Unit	Lessons learned list	
	Closure Unit	Formal closure certificate	

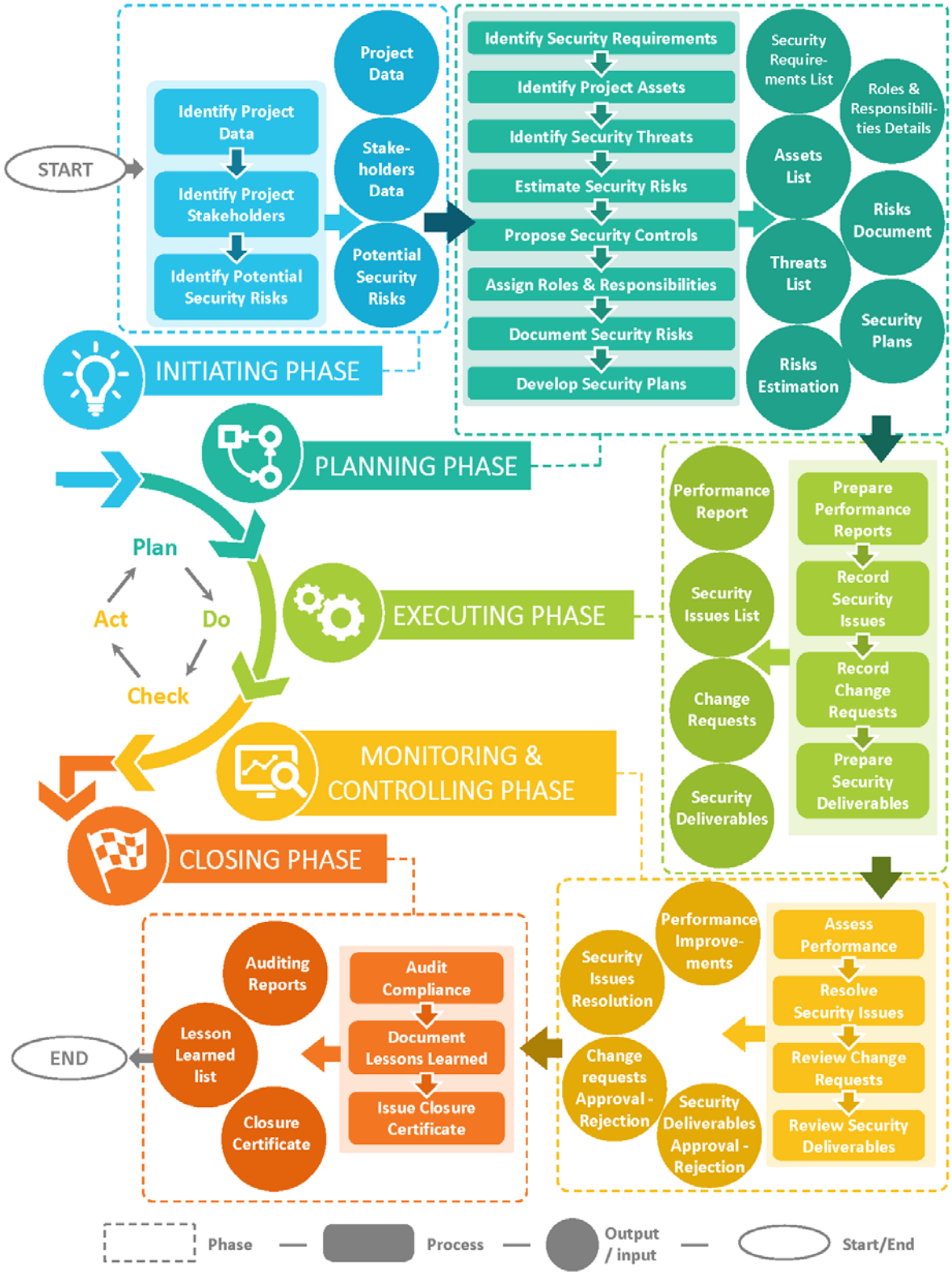

Figure 5.2: OSCR Framework Workflow

The following sub-sections detail the OSCR framework components and explain how it works using the API/PNR case study.

5.2.1 Initiating Phase

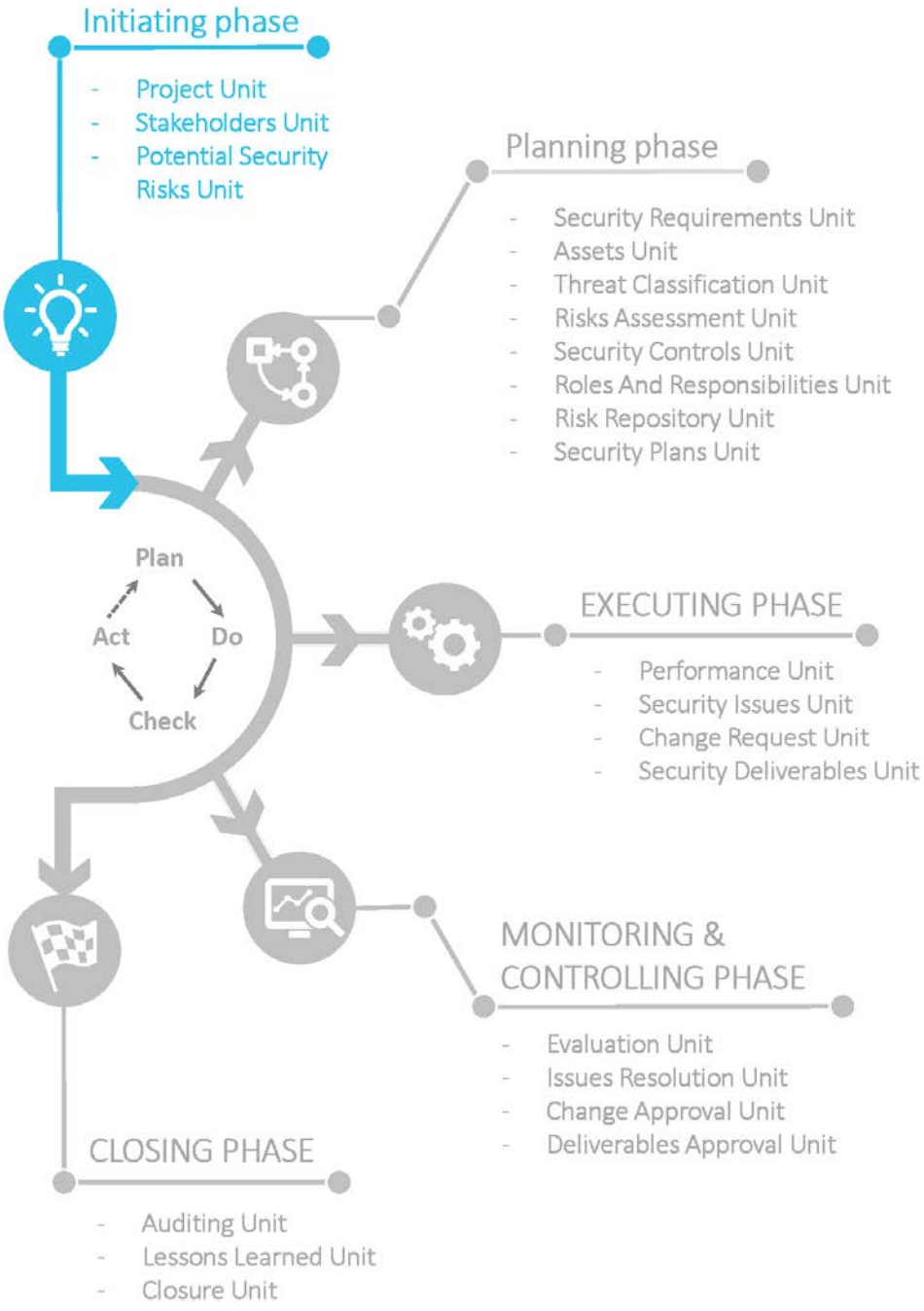

Figure 5.3: Initiating Phase

The aim of this phase is to establish the project's unique data, and identify the main project stakeholders and general security risks to which the project might be exposed. The client is responsible for this phase, as no provider has yet been selected. This phase achieves its objectives through the following units:

5.2.1.1 Project Unit

This unit handles all of the project's essential data. If the project is new, the client uses this unit to produce the project data details such as project ID, name, code etc. If the project already exists, the client can update any project details, if there is a need for such an update. The project ID will be the primary key, used to distinguish the project from other projects. All security risks and plans, or any other security works related to this project, will use the unique project ID. If the client has a Project Management Office (PMO), then the project unit should be produced and managed by the PMO team. If not, then the projects department or any other department should be responsible for the project unit. In our case study (API/PNR), the output of this unit is presented in Table 5.2.

Table 5.2: Project Essential Data

Project ID	1	Project Code	API/PNR
Project Name	Advanced Passenger Information/Passenger Name Record		
Project Type	Web Application		
Project Start Date	01/01/2012		
Project End Date	01/01/2017		
Project Duration	60 Months		
Project Owner	Moneef Almutairi		
Project Provider	XYZ Company (if it is known)		
Project Manager	Thomas Marten (if it is known)		
Project Cost	$ 100000000		

5.2.1.2 Stakeholders Unit

The aim of this unit is to identify the project stakeholders who will be involved in the project. If security risks are to be managed appropriately, it is essential to firstly identify all the parties involved in the project implementation, and secondly to identify their roles and responsibilities in the project execution. It

should be noted that stakeholders' roles and responsibilities differ based on their level of involvement in the project execution. Some stakeholders might be involved in executing some security plans partially or totally developed by the project team, whereas other stakeholders may receive some security awareness sessions only.

Table 5.3 presents an example of the stakeholders of the API/PNR project.

Table 5.3: Stakeholders' Data

Project ID	1	Project Code	API/PNR
Stakeholders' Data			
Stakeholder Name	Stakeholder Type	Stakeholder Role	
General Immigration Directorate	Government Sector	End user	
Security Affairs Directorate	Government Sector	General background check of outsourced staff	
General investigation Directorate	Government Sector	Watch list administrator	

5.2.1.3 Potential Security Risks Unit

The aim of this unit is to identify potential security risks that might take place while executing the project. These potential security risks are identified by the client's staff working in the security department, or they can be derived from the historical data of similar projects. Although the output of this unit is not a comprehensive security analysis, it gives the client's decision makers a general overview of the potential security risks that the organisation might face as a result of executing this project. Based on this overview, the decision makers can decide whether to implement this project or not, or to implement appropriate security controls before implementing the project. In our case study, the potential security risks can be similar to the ones in Table 5.4.

Table 5.4 : Potential Security Risks

Project ID	1	Project Code	API/PNR
Potential Security Risks			
RISK ID	Risk Description		
1	Information disclosure by provider's staff		
2	DoS attacks		
3	Unauthorised data centre access by provider's staff		
4	Malware and Virus		
5	SQL injection attack		
6	Spoofing		

5.2.2 Planning Phase

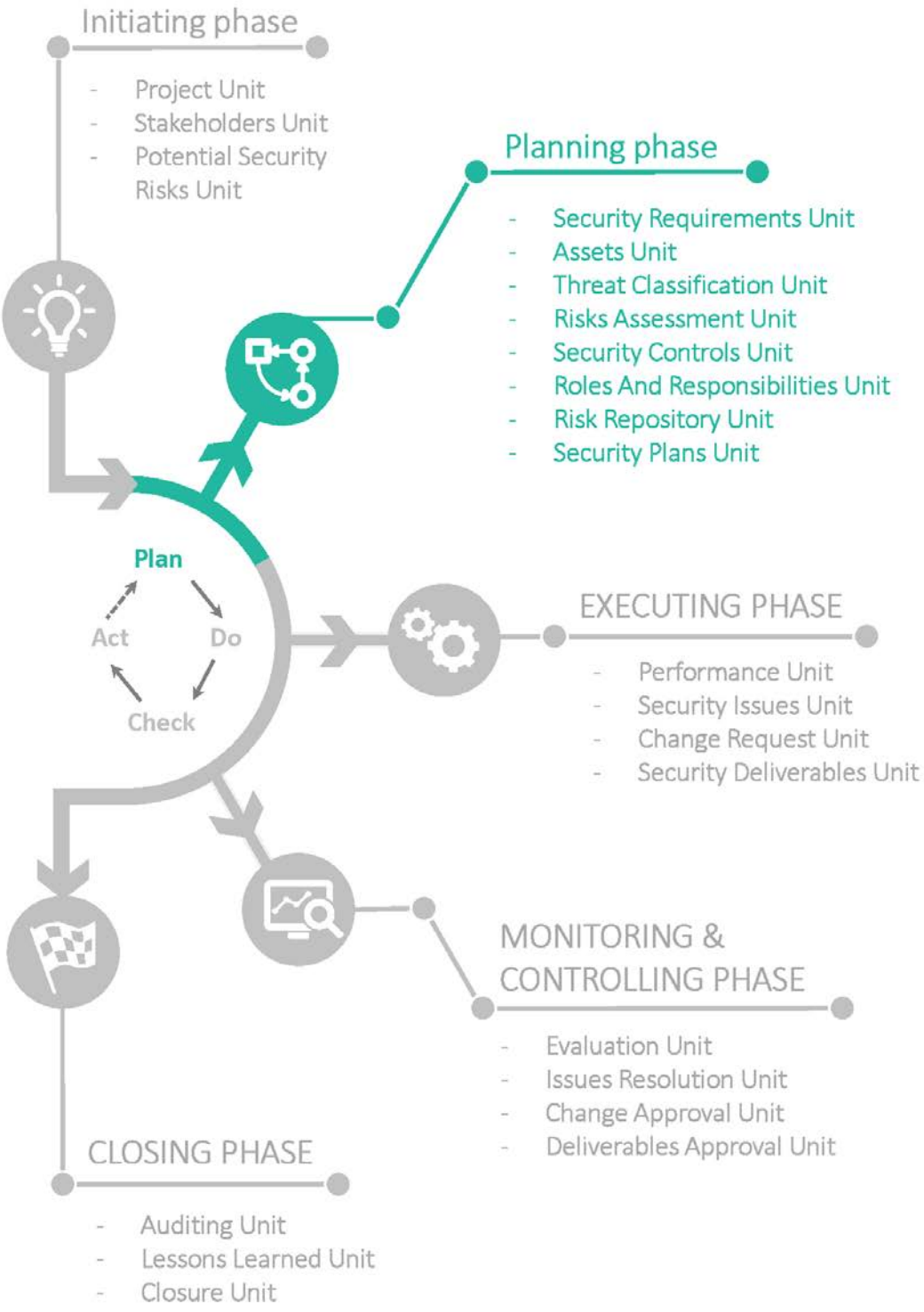

Figure 5.4: Planning Phase

The planning phase, which represents the (Plan) stage of the PDCA model, is the core part of the OSCR framework. The main parties involved in the project execution carry out all of the core security activities at this phase. The primary parties are the client and the provider. If other stakeholders are involved in executing security activities, then they participate with the primary parties in preparing the required security analysis and plans. The following sub-sections describe the planning phase units in more detail:

5.2.2.1 Security Requirements Unit

The aim of this unit is to clearly identify the security requirements of the project. Without clear security requirements, security analysis and plans may not achieve their goals properly. The first step in identifying the security requirements is to refer to what has been written by the client in the Request For Proposal (RFP) with regard to security requirements. However, the security requirements in the RFP might have been changed over time. To make sure that security requirements are up to date, the provider needs to review them with the client's related departments. This can be done through workshops or direct meetings. When the review of security requirements is complete, the provider must document them and both parties, the client and the provider, need to sign the document, which represents the output of this unit. Example of API/PNR security requirements are presented in Table 5.5.

Table 5.5: Security Requirements

Project ID	1	Project Code	API/PNR
Security Requirements			
Requirement ID	Requirement Description		
RQ-1	All messages outside the client's private intranet must be encrypted		
RQ-2	The system must provide extensive auditing capability, able to record all users and system events		
RQ-3	The system must ensure the confidentiality of the client and the system information		

Project ID	1	Project Code	API/PNR
Security Requirements			
Requirement ID	Requirement Description		
RQ-4	The availability of the system must achieve 99.999%.		
RQ-5	The system must support role-based access control		
RQ-6	The system must maintain the privacy and security of traveller data		
RQ-7	The system must be designed to support zoning architecture to separate traffic		
RQ-8	The system must be backed up regularly according to the client's backup policy		

5.2.2.2 Assets Unit

One crucial step towards managing the security of outsourced IT projects is asset identification and categorisation. Without knowing what needs to be protected, it might be difficult to identify potential security threats, and to select the right security countermeasures to mitigate their impact.

The first step in this unit is identifying all assets that will be delivered or affected by the project. The second step is to categorise the assets into groups. Identifying security threats for each asset might be challenging and time consuming as large projects usually involve a huge number of assets. Hence, categorising them into groups decreases the complexity and difficulty of identifying all threats for each asset. However, if the number of assets is not large and resources are available, all assets should be identified. The project assets can be categorised into the following groups [18, 156]:

- Software: this includes all applications that will be included in the project's execution.
- Hardware: this includes all hardware (servers, PCs, etc.) that will be included in the project's execution.
- Network: this includes all network devices such as switches, routers, communications and firewalls that will be included in the project's

execution. It should be noted that network devices can be included in the previous group, but have been excluded to better allow the network team, which is usually a different department from the hardware (servers, hosts, PCs, etc.) department, to concentrate on and manage the security risks related to their department's assets (network assets).

- Information: this includes all data that will be processed by the project or any information produced or stored by the project.

Table 5.6 provides an example of the project assets for the APP/PNR project.

Table 5.6: Project Assets

Project ID	1	Project Code	API/PNR
Project Assets			
Asset Type	Asset ID	Asset description	
Hardware	HW-1	HP 7000 Blade enclosure	
	HW-2	HP BL460c Blades	
Software	SW-1	Apache Web Server	
	SW-2	Apache Tomcat Application Server	
	SW-3	Redhat linux	
	SW-4	I2 Analyst Notebook	
Network	NW-1	Cisco ASA 5520 Firewall	
	NW-2	Cisco Load Balancer	
	NW-3	Cisco Layer 3 Switch	
Information	IN-1	Traveller information	
	IN-2	The client's information	

5.2.2.3 Threat Classification Unit

Bearing in mind the limitations of existing threat classification approaches explained in the previous chapter, such as the lack of using exhaustive criteria and the lack of consideration of the desired properties, we propose a new hybrid thread classification approach (called the outsourcing threat classification approach) for identifying security threats in an outsourcing context. The outsourcing classification approach combines different threat classification criteria and takes into consideration the desired properties that good threat

classification approaches should have (discussed in Chapter 4). It is a systematic and comprehensive approach that takes into account threats from different perspectives such as external threats, provider threats, client threats, physical and environmental threats. The threat classification criteria that we use in the outsourcing threat classification approach are shown in Figure 5.5, and described as follows:

- Threat Source: the origin of the threat, which can be external threats, client threats, provider threats, or environmental and physical threats.
- Threat agent: the agent that causes the threat. This can be technical, human, or organisational.
- Asset type: the type of asset impacted by this threat. It can be networks, software, hardware or information.
- Threat intention: the type of human behaviour that caused the threat. It can be accidental or intentional.
- Environmental and physical threat type: the type of environmental and physical threat. It can be controlled or non-controlled.
- Threat impact: the result of the threat on the information system. It can affect the confidentiality, integrity or availability (C-I-A).

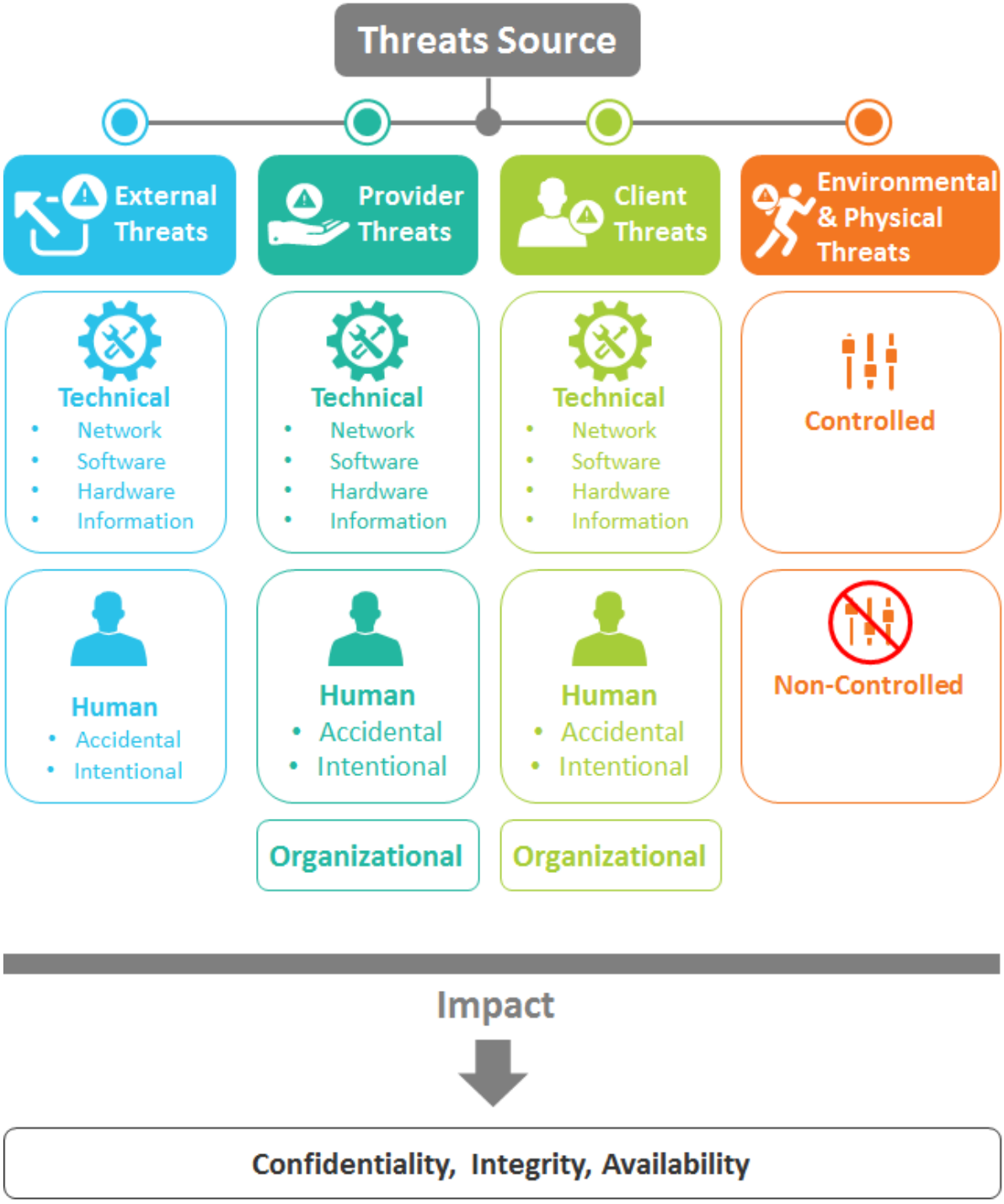

Figure 5.5: Outsourcing Threat Classification

In the outsourcing context, where different parties are involved in the project's execution, we suggest that the source of threats can be one of four: external attackers, the provider itself, the client, and environmental and physical threats. The results of any threat from any source could lead to major security risks involving confidentiality, integrity or availability.

External threats are either technical or human. Technical threats are those that target one or more of the project's or organisation's assets. They can target the network, software, hardware, or information assets. Such threats employ technology (e.g. the internet) to attack the project and organisational assets. Human threats might be accidental or intentional and they represent threats that are imposed by non-technical actions such as accessing buildings and collecting sensitive information without permission. This can be similar to our case study external threats shown in Table 5.7.

Table 5.7: External Threats

<table>
<tr><td colspan="2">Project ID</td><td>1</td><td>Project Code</td><td>API/PNR</td></tr>
<tr><td colspan="3">External Threats</td><td>Impact</td></tr>
<tr><td rowspan="15">Technical</td><td></td><td colspan="2"></td><td rowspan="20">C-I-A</td></tr>
<tr><td colspan="2">Software:</td><td></td></tr>
<tr><td></td><td colspan="2">Malware and virus</td></tr>
<tr><td></td><td colspan="2">SQL injection attack</td></tr>
<tr><td></td><td colspan="2">Intellectual property theft</td></tr>
<tr><td colspan="2">Hardware:</td><td></td></tr>
<tr><td></td><td colspan="2">Denial of service attack</td></tr>
<tr><td></td><td colspan="2">Hardware destruction</td></tr>
<tr><td colspan="2">Network:</td><td></td></tr>
<tr><td></td><td colspan="2">IP spoofing</td></tr>
<tr><td></td><td colspan="2">Packet sniffing</td></tr>
<tr><td></td><td colspan="2">Session hijacking</td></tr>
<tr><td colspan="2">Information:</td><td></td></tr>
<tr><td></td><td colspan="2">Information intercept</td></tr>
<tr><td></td><td colspan="2">Phishing</td></tr>
<tr><td rowspan="4">Human</td><td colspan="2">Accidental:</td><td></td></tr>
<tr><td></td><td colspan="2">Information disclosure</td></tr>
<tr><td colspan="2">Intentional:</td><td></td></tr>
<tr><td></td><td colspan="2">Unauthorised data or document collection</td></tr>
</table>

The provider threats category represents threats that are imposed by the provider who executes the project. Provider threats are divided into three categories: technical, human and organisational. Technical threats represent threats that affect one or more of the project's or client's assets. They can affect the network, software, hardware or information assets. Such threats use

technology to affect the assets (e.g. software bugs). Human threats might be accidental or intentional and they represent threats that are imposed by non-technical actions such as accessing client data centres without permission and collecting sensitive information about the client. The organisational threats represent threats imposed by a lack of adequate security procedures and processes (e.g. lack of security policies), which might impose security threats on both the client and the provider. An example of provider security threats for API/PNR project is presented in Table 5.8.

Table 5.8: Provider Threats

Project ID	**1**	**Project Code**	**API/PNR**
Provider threats			**Impact**
Technical			C-I-A
	Software:		
		Lack of event logs	
		Malware and virus	
		Application bugs	
		Improper authentication	
	Hardware:		
		Un-patched servers	
		Faulty hardware	
	Network:		
		Usage of default configuration	
		Unencrypted messages	
	Information:		
		Information destruction	
		Information tampering	
Human	Accidental:		
		Information disclosure	
		Human error	
	Intentional:		
		Neglecting security policies	
Organisational		Lack of business continuity management	
		Lack of disaster recovery planning	
		Lack of configuration management	
		Lack of incident management	

The third category is client threats. This category has greater importance, especially when there is any type of integration with the client's existing systems.

Such integration might affect the confidentiality, integrity or availability of the client's existing systems. The client threats contain the same categories as the provider threats. This category is designed to overcome the limitations of some existing threat classification approaches that do not take into consideration insider security threats. For our case study, this can be similar to the threats presented in Table 5.9.

Table 5.9: Client Threats

Project ID	**1**	**Project Code**	**API/PNR**
Client threats			**Impact**
	Software:		C-I-A
		Integration bugs	
		Unauthorised resources access	
	Hardware:		
		Hardware failure	
		Hardware obsolescence	
	Network:		
		Lack of anti-virus	
		Usage of default configuration	
		Lack of intrusion detection systems	
	Information:		
		Information destruction	
		Information intercept	
		Information tampering	
Human	Accidental:		
		Information disclosure	
		Accidental bad data entry	
	Intentional:		
		Neglecting security policies	
Organisational		Improper hardware and data disposal	
		Inadequate assets management	

The fourth category is environmental and physical threats. This category represents threats that arise from the environmental and physical conditions. These threats might be controlled, such as controlling the temperature of the data centre, or uncontrolled, such as earthquakes. Table 5.10 presents an example of environmental and physical threats for API/PNR project.

Table 5.10: Environmental & Physical Threats

Project ID	**1**	**Project Code**	**API/PNR**
Environmental & Physical Threats			**Impact**
Controlled:	Lack of temperature controlling system		C-I-A
	Lack of fire resistance system		
	Lack of redundant electricity power		
Non-Controlled:	Earthquakes		
	Flood		
	Terrorism		

5.2.2.4 Risk Assessment Unit

The ultimate aim of this unit is to estimate and prioritise potential security risks' impacts on project assets. The risk assessment unit has five steps: vulnerabilities identification, risk likelihood determination, risk magnitude determination, risk estimation and risk prioritisation [19, 157]. These five steps are described as follows:

- Vulnerabilities identification: Vulnerabilities do not harm the information system by themselves, but they might be exploited by threats to damage the information system or they might cause undesired effects on it [158]. Therefore, it is essential to identify all vulnerabilities that might be used by the threat sources identified in the previous section.
- Risk likelihood determination: the OSCR framework divides the likelihood of the risk into five number ranges (0-20, 21-40, 41-60, 61-80 and 81-100). These ranges represent five level values – very low, low, moderate, high and very high, respectively. Table 5.11 shows the threat likelihood values and their description for the OSCR framework [19].

Table 5.11: Threat Likelihoods

Qualitative Values	Categories	Description
Very High	81-100	Almost certain that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).

Qualitative Values	Categories	Description
High	61-80	High likely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).
Moderate	41-60	Somewhat likely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).
Low	21-40	Unlikely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).
Very Low	0-20	High unlikely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).

- Risk magnitude determination: In a similar way to the risk likelihood categories, the magnitude or impact of the risk is divided into five number categories (1, 2, 3, 4, and 5), which represent five level values – minor, moderate, major, critical and severe, respectively. Table 5.12 shows the threat impact values and their description for the OSCR framework [19].

Table 5.12: Threat Impacts (magnitudes)

Qualitative Values	Categories	Description
Severe	5	Multiple severe or catastrophic impacts on the project or organisational assets if the threat occurs.
Critical	4	Severe or catastrophic impact on the project or organisational assets if the threat occurs.
Major	3	Serious impact on the project or organisational assets if the threat occurs.
Moderate	2	Limited impact on the project or organisational assets if the threat occurs.
Minor	1	Negligible impact on the project or organisational assets if the threat occurs.

- Risk estimation: In the OSCR framework, we will use a semi-quantitative method to estimate the security risks of outsourced IT projects, as shown in Table 5.11 and Table 5.12. This will allow

decision makers to understand risk assessment results easily and it will also help risk assessors to assess risks more accurately and to interpret them as an understood value (e.g. 80 interpreted as high). We will also use the ordinary Risk Exposure (RE) equation, which has been used in many risk assessment analyses for risk estimation. In the RE equation, the risk exposure is the result of the likelihood multiplied by the magnitude (the impact) of the risk. The RE equation is used as follows:

$$RE = likelihood * magnitude$$

Following the above guidance and explanation, security risks can be estimated easily using the risk exposure equation. For instance, in the APP/PNR case study, if we take a web server as an example of a project asset, and a Denial of Service (DoS) attack as an example of a threat to that asset, and if we assume that there are no intrusion detection systems in place, we can estimate the risk exposure as shown in Table 5.13.

Table 5.13: Risk Estimation

Project ID	1	Project Code	APP/PNR
Risk ID	R2		
Asset Type	Hardware		
Asset ID	HW-1		
Asset Name	Web server 1		
Threat	DoS		
Threat source	External threat		
Vulnerability	Lack of intrusion detection systems		
Risk Likelihood	0.95		
Magnitude	4		
Risk Exposure	0.95 * 4 = 3.80		

- Risk prioritisation: the last step in this unit, but by no means the least important, is to prioritise the risks estimated in the previous step. The aim of this step is to allow project teams to concentrate on the risks that potentially have the highest impact on the confidentiality, integrity and availability of project assets. Table 5.14 shows a

representative example of the risk prioritisation of the APP/PNR project.

Table 5.14: Risk Prioritisation

Project ID	1	Project Code	API/PNR
Risk ID	Threat Source	Risk Description	RE
R1	External Threat	Malware and virus	4.5
R2	External Threat	DoS	3.80
R3	Client Threat	Information disclosure	3.6
R4	Provider Threat	Unencrypted messages	3.2
R5	External Threat	SQL injection attack	3
R6	Environmental & Physical Threats	Terrorism	2.5
R7	Provider Threat	Improper authentication	1.8
R8	Provider Threat	Application bugs	1.8
R9	Client Threat	Usage of default configuration	1.6
R10	External Threat	Unauthorised building access	1.2
R11	Provider Threat	Un-patched servers	0.6
R12	Provider Threat	Faulty hardware	0.2

5.2.2.5 Security Controls Unit

Having identified the threats of outsourced IT projects, and after assessing and prioritising the risks associated with these threats, the project team needs to plan security controls (countermeasures) that can mitigate such security risks. Countermeasures answer the question of how to protect project assets.

Security countermeasures should mitigate security risks in a cost-effective and efficient way that helps to achieve confidentiality, integrity and availability. Not all organisations are able to implement security countermeasures at any cost, but they aim to implement countermeasures that mitigate the security risks efficiently, within the organisation's cost boundaries [20, 159].

Security countermeasures are not only technical; other countermeasures such as organisational and human play an important role in achieving security goals. Therefore, the OSCR framework categorises security countermeasures into three groups: technical, organisational and human [20, 159, 160]:

- Technical countermeasures: technical solutions that aim to mitigate security risks. Technical solutions might be designed for controlling hardware, software, network or information risks. Examples of technical countermeasures include cryptography, intrusion detection systems and role-based access controls.
- Organisational countermeasures: represent controls that are designed to mitigate non-technical security risks. They are administrative and legal activities that facilitate building secure and protected environments. Examples of organisational countermeasures include security polices, contracts, and audit and compliance processes.
- Human countermeasures: activities designed to educate, train, motivate, and improve the security awareness of employees, in order to help achieve the organisation's security goals.

Table 5.15 shows an example of security countermeasures for the APP/PNR case study.

Table 5.15: Security Countermeasures

Project ID	1	Project Code	API/PNR
Risk ID	Countermeasure Type	Security Countermeasures	
R1	Technical	Anti-virus	
R2	Technical	Intrusion detection system, firewalls	
R3	Organisational	Non-disclosure agreement	
R4	Technical	Cryptography	
R5	Technical	Anti-virus, intrusion detection system, firewalls	
R6	Organisational	Disaster recovery site	
R7	Technical	Role-based access control	
R8	Human	Training	
R9	Technical	Disabling of unused ports	
R10	Organisational	Physical access control, CCTV	
R11	Technical	Regular updates	
R12	Technical	Prior production tests	

5.2.2.6 Roles and Responsibilities Unit

The aim of this unit is to assign security activities to project teams using a clear method that helps to prevent any ambiguities between the project teams, especially if the client and stakeholder teams are involved.

In the OSCR framework, we propose a role-based RACI method for assigning the roles and responsibilities of project security activities. The role- based RACI suits the context of outsourced projects, as their resources are not stable and they might play a part in the project activities in specific phases only (e.g. planning phase) [161]. However, if the project is large and further breakdown is required, name-based RACI can be used to complement the role-based RACI. Table 5.16 provides a representative example of our proposed RACI for the API/PNR project.

Table 5.16: Roles and Responsibilities

Project ID	1		Project Code		API/PNR
Security Activity	Project Owner	Project Manager	Business Analyst	Security Architect	Development Team
Security requirements	I	A	R	I	I
Project assets	I	A	I	R	C
Threat classification	I	A	I	R	C
Risk assessment	I/A	R	C	C	I
Security controls	I	A	C	R	C
Intrusion detection system implementation	I	A	I	R	C
Cryptography	I	A	I	C	R
Role-based access control	I	A	I	C	R
Non-disclosure agreement	A	R	I	I	I
Prior production tests	I	A	R	I	C

5.2.2.7 Risk Repository Unit

Risks that have been identified, assessed, and prioritised during the planning phase or any later phases of the project execution need to be documented and

made available for project members' access whenever needed. The risk repository unit achieves this aim and contains all the project security risks that have been identified so far. Any risk that has been logged into the risk repository unit should have sufficient information about that risk, such as risk ID, description, impact, asset name and so on. This information allows the project members to have a full understanding and awareness of all the potential security risks, even if they are not specialised in security. Table 5.17 provides a representative example of a risk repository unit entry.

Table 5.17: Risk Repository Entry

Project ID	1	Project Code	APP/PNR
Risk ID	R2		
Asset Type	Hardware		
Asset ID	HW-1		
Asset Name	Web server 1		
Threat	DoS		
Threat Source	External threat		
Vulnerability	Lack of intrusion detection systems		
Risk Likelihood	0.95		
Magnitude	4		
Risk Exposure	0.95 * 4 = 3.8		
Risk Description	Web server 1 might be affected by DoS attack leading to unavailability of services provided by this sever		
Impact on Security	Availability		
Security Controls	Use of intrusion detection system		

5.2.2.8 Security Plans Unit

The planning phase in the OSCR framework ends with the security plans unit. This unit is responsible for developing security plans that will be used to achieve the project's security goals and thus contributes to building a secure and protected environment. As they vary from one organisation to another for several reasons (e.g. infrastructure design, assets importance, cost) the contents of these plans are outside the scope of this research. Security plans in this unit may include the following, which represent an example of API/PNR security plans:

- Information security policy.

- Communications and operations management plan.
- Access control plan.
- Information systems acquisition, development, and maintenance plan.
- Asset management plan.
- Incident management plan.
- Business continuity management plan.

Outsourced IT projects vary in their objectives, assets, threats, risks and so on. Therefore, security plans developed in this unit should take into consideration this variation and design the required security plans (e.g. business continuity plan) so that they suit the project's context and objectives.

5.2.3 Executing Phase

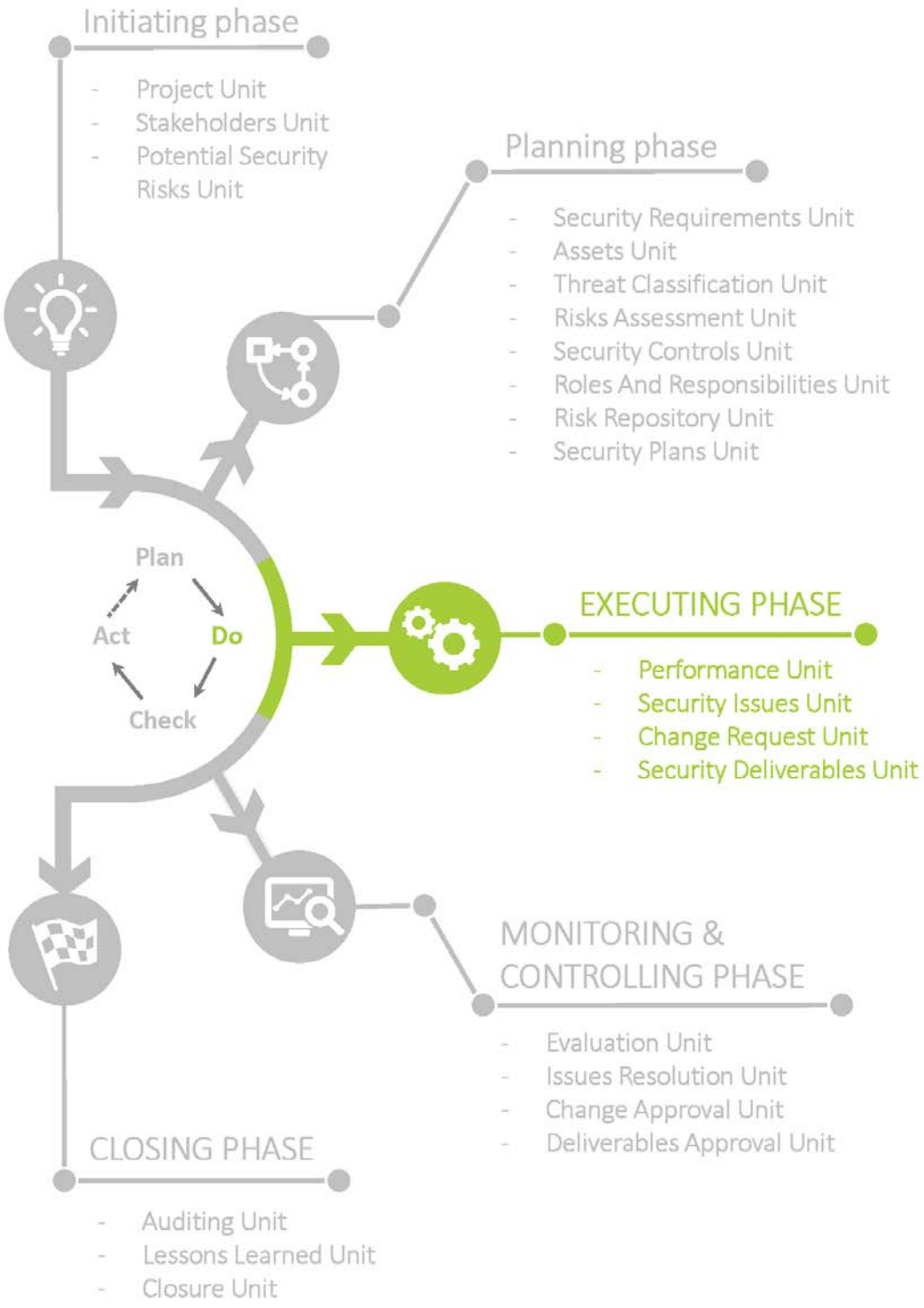

Figure 5.6: Executing Phase

In this phase, which represents the (Do) stage of the PDCA model, the security plans and controls that were proposed in the previous phase are put into practice. Any security issues that might be experienced are documented and monitored. If there is any need for improvements or changes, the project team will record that. The executing phase achieves its objectives through the following units:

5.2.3.1 Performance Unit

While project personnel engage in executing security activities, they assess the performance and report any issues to the management team. The project manager monitors and assesses project teams' performance with regard to security activities. If there is any deviation from what has been planned, the project manager should take corrective actions. The deviation might result from a lack of clarity in security plans, or a lack of personnel skills. Regardless of the reason, the project manager is responsible for resolving any deviation. All performance reports should be documented and shared with the project steering committee, which should include a project sponsor, program manager, security expert and PMO officer from the client. It should also include a program manager and security consultant from the provider. The main responsibility of the project steering committee is to provide support to the project manager and resolve any project issues.

5.2.3.2 Security Issues Unit

Not all security activities, controls, and plans work as planned. Different issues might be experienced by the project. Technologies keep changing over time and what might work effectively today could not meet tomorrow's expectations. Other circumstances might contribute to security issues. The complexity of environments might lead to conflict and affect the desired security goals that the project teams seek. Changes in client environments or security requirements are examples of causes that could lead to various security issues. The project teams should assess these issues and take corrective actions. Whatever the reasons for

security issues, they must be documented by the project manager through this unit.

5.2.3.3 Change Requests Unit

The aim of this unit is to record all security change requests raised by the project manager. If security issues recorded in the previous unit cannot be resolved without making changes to what has been planned, then a change request must be raised by the project manager through this unit. It is designed to control changes and to allow the provider and client to agree on a new plan that suits all parties, and, more crucially, one that achieves the desired security goals. Moreover, not all new plans can be implemented with the same cost; extra funds might need to be allocated by either the provider or the client. The new security plans might also conflict with other security plans and controls, which explains why this unit is needed.

5.2.3.4 Security Deliverables Unit

The execution of the project involves achieving project deliverables according to the agreed master schedule. Security deliverables should be monitored by the project manager to avoid any delay. The delay in achieving project deliverables, regardless of whether or not they are security deliverables, might lead to penalties. When security deliverables are achieved, they must be reviewed by the project manager to make sure that they meet the project and client's requirements. If they meet the agreed requirements, then they are recorded in this unit and will be signed later on by all parties.

5.2.4 Monitoring and Controlling Phase

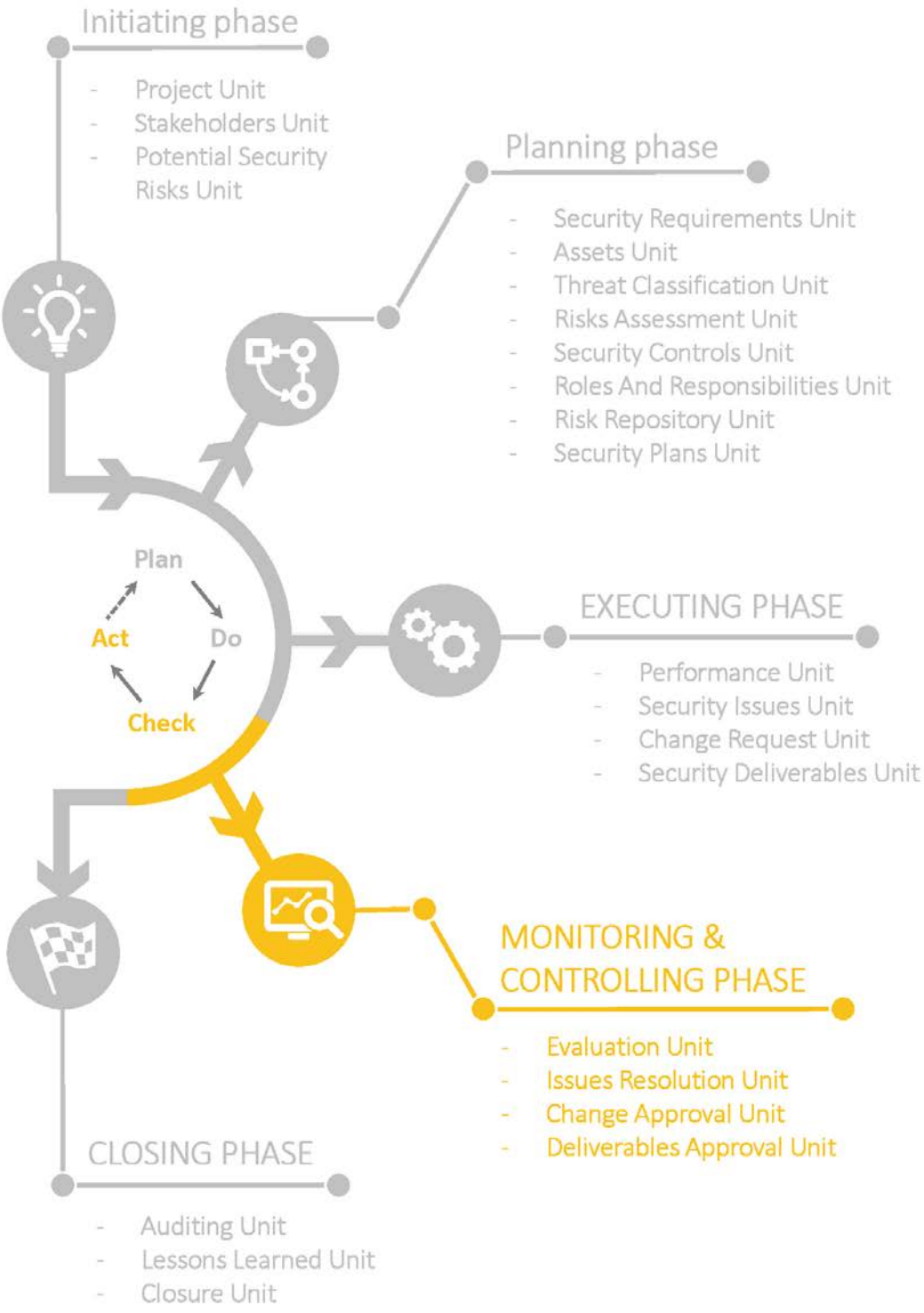

Figure 5.7: Monitoring & Controlling Phase

The project execution needs to be monitored and controlled not only by the project manager, but also by the project steering committee, to make sure that it meets its requirements and to provide all the support required for project execution so that it achieves its security and non-security goals. The aim of this phase, which represents the (Check) and (Act) stages of the PDCA model, is to evaluate the execution performance reports, and assess if there is any need for improvements. Moreover, the project steering committee supports the project manager in resolving security issues that require their intervention. Security change requests and security deliverables are reviewed and approved or rejected at this phase too. The monitoring and controlling phase has the following units:

5.2.4.1 Evaluation Unit

As mentioned in the previous phase, the performance of project execution, including security activities and plans, is monitored and documented by the project manager and their teams. All performance reports are documented through the performance unit. Those reports are reviewed and assessed at this phase through the evaluation unit. Based on this review, the project steering committee may propose some improvements that could help to achieve project security goals in an effective and efficient way. If the performance is good and there is no need for any improvement, then the steering committee signs off existing performance reports.

5.2.4.2 Issues Resolution Unit

The aim of this unit is to resolve security issues that might be experienced during the project's execution. Security issues resolution might be beyond the ability of the project manager (e.g. client environment change). Therefore, intervention from the project steering committee might help to resolve some security issues. It should be noted that some security issues might already have been resolved by the project manager and their teams, but they are still recorded in order to allow the project steering committee to be up to date with all security issues.

5.2.4.3 Change Approval Unit

Changes in security requirements, controls, or plans need to be approved by the client and the provider. These changes might lead to other impacts such as project security controls, budget increase or schedule extension. Therefore, the aim of this unit is to allow the project steering committee to analyse these changes and assess their potential impacts on the project. If these changes can be tolerated by both parties, then they approve them. However, approved changes may require the project team to update other security controls or plans in order to avoid any conflict that might lead to new security issues.

5.2.4.4 Deliverables Approval Unit

The project security deliverables are planned according to the agreed master schedule. All project deliverables that meet the client's requirements were reviewed and documented by the project manager in the previous phase. The aim of this unit is to review and approve, or reject, the deliverables that have been achieved so far. This review and approval, or rejection, is carried out by the project steering committee. Any rejected security deliverable goes back to the project manager who updates the deliverable based on the steering committee comments and then the deliverable undergoes the same process again.

5.2.5 Closing Phase

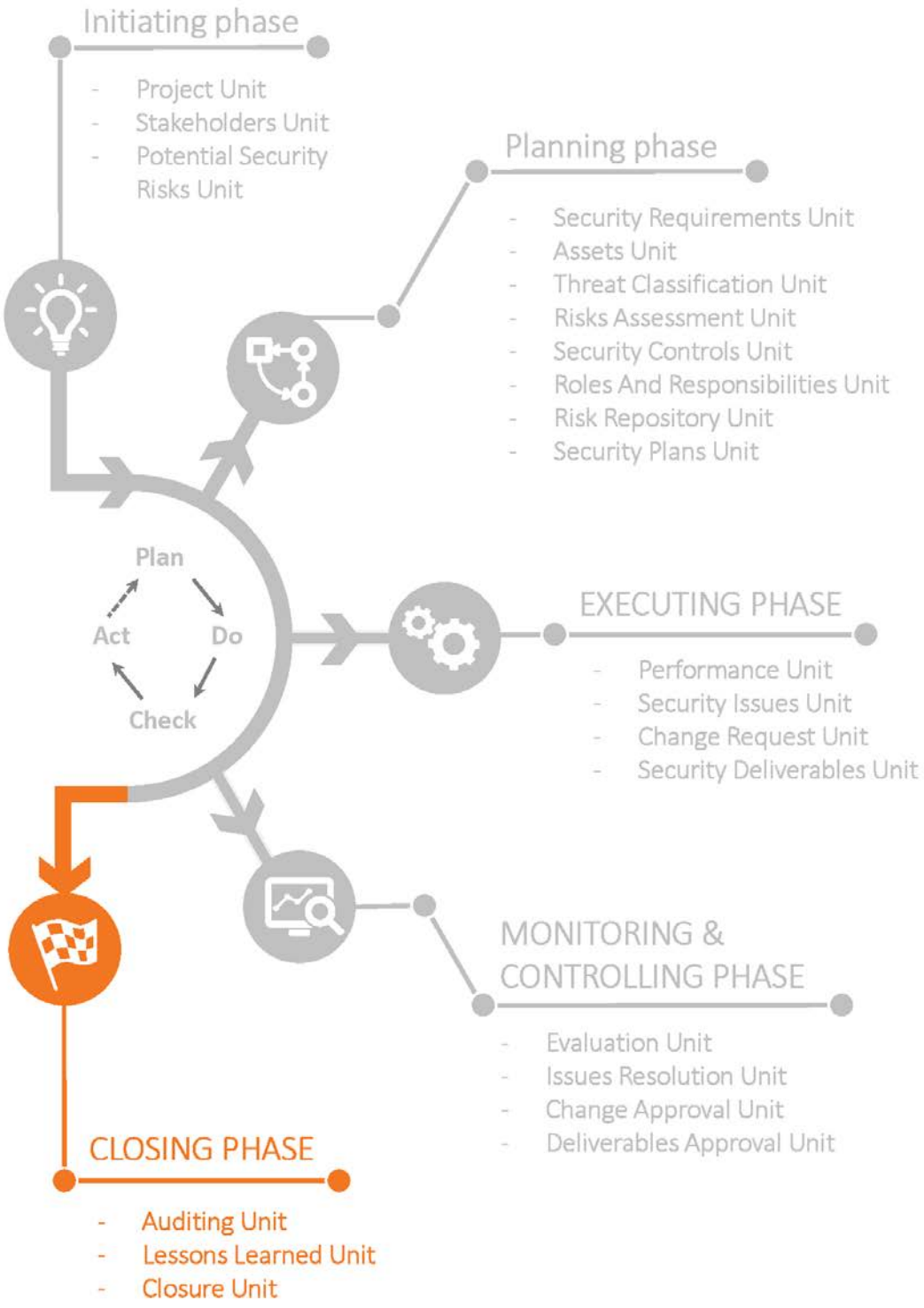

Figure 5.8: Closing Phase

When the project execution comes to the end, the project will be handed over to the client. Before the client takes control, the project requirements, including the security requirements, need to be verified to make sure that the project has achieved its security and non-security goals. The aim of this phase is to audit and verify the project requirements in order to close the project officially and issue the provider with the project closure certificate. Moreover, the lessons learned during the project phases are documented at this phase for future use. The closing phase has the following units:

5.2.5.1 Auditing Unit

Security requirements that have been agreed by both parties, the client and provider, need to be validated and assessed before the transition of the project starts. The aim of this unit is to demonstrate that the applications or the products being delivered by the project are secure and that they work according to the requirements agreed in the project scope of the work. The validation and assessment may use different techniques based on the type of services being delivered by the project. Check lists or reviewing the project security deliverables and documents are examples that can be used for security auditing. Another example is penetration tests that can be used to demonstrate whether the project deliverables (e.g. applications, products) are secure as claimed or not. Vulnerabilities assessment is another example of project auditing that can help to evaluate the level of security risks that might be involved in the project products.

5.2.5.2 Lessons Learned Unit

Mistakes are not always detrimental; sometimes they prevent organisations from repeating similar mistakes. It is important to document all lessons learned during the project execution. This is more important for organisations where outsourcing represents an integral part of their business. Such lessons could help organisations to avoid similar mistakes with future projects, which will help them to save their resources. Lessons learned should not be only mistakes;

positive actions that could have a significant impact on the security of the project should be taken into consideration as well. Whatever the type of project lesson learned, they should all be documented for future use through this unit.

5.2.5.3 Closure Unit

The last step in the OSCR framework is to close the project formally. The client will have to issue the provider with a project closure certificate. By issuing this certificate, the client and all stakeholders involved in this project agree that the project has completed all its requirements and achieved its objectives. Moreover, responsibility for the project is transitioned officially to the client. As a result, the project is closed and the contract comes to an end.

5.3 Analysis

To manage the security and compliance risks in the outsourcing context effectively, we have proposed the OSCR framework. It is designed to provide a comprehensive methodology that provides organisations with the ability to minimise, mitigate or eliminate security risks in the early stages of project execution. The OSCR framework uses a hybrid threat classification approach that has been designed for the outsourcing context. It is designed to overcome the lack of exhaustive criteria limitation of existing threat classification approaches. Threats are considered from different perspectives to be able to identify all the potential security threats that the project might face.

The OSCR framework is an asset-based approach that allows the framework to be independent from different constraints such as project size, type or time. The asset-based approach addresses variation in security requirements from one organisation to another as the approach is not a 'one size fits all' approach. It identifies assets that will be delivered by the project, assesses the security risks related to these assets, and proposes the appropriate security controls.

Many project management and software development approaches, such as Waterfall and Agile, have been developed and adopted by different organisations.

The Waterfall model is a sequential development process, in which progress comes to existence through specific phases (requirements, design, development, testing and maintenance). The requirements should be clear (and remain unchanged in all phases) before moving to the design phase. The implementation based on this model is easy as it is a linear model and the resources required are minimal. Agile is an iterative methodology in which requirements are delivered iteratively and incrementally throughout the project life cycle. The requirements can be changed and customers' satisfaction is achieved through quick and continuous delivery of small and working pieces of software [162, 163].

While existing project management and software development approaches, such as Waterfall, Agile, etc., concentrate on the principles and processes that can be used to improve the software development process, the OSCR concentrates on the security and compliance processes that can be used to avoid or mitigate security risks when outsourcing. Although the OSCR framework uses specific phases, it is built upon the PDCA model, which allows the OSCR framework to overcome the limitation of Waterfall in responding to requirement changes. While the benefits of Agile can be seen more obviously in small projects and the required knowledge to implement it is high, the OSCR framework is independent from different constraints, such as the project size or time, and can be followed with fundamental knowledge of security management [162, 163]. The main features of the OSCR framework are summarised as follows:

- Provides a systematic and comprehensive approach for managing the security and compliance risks when IT projects are outsourced. It takes into account all of the parties involved in the completion of the project's execution, such as providers, the client and stakeholders.
- It is a structured approach, which uses project phases to manage and control project security risks.
- The Plan-Do-Check-Act model that the OSCR framework is built upon allows flexibility. The teams that are managing the security risks are

able to constantly oversee and assess the security controls and are therefore quickly able to execute any required improvements.

- The OSCR framework is easy to use. Security risks can be managed separately in each project phase.
- The OSCR framework is an asset-based approach that provides a general approach, meaning that it is suitable for projects of any size or type.
- Compliance with security requirements and controls is enforced throughout the project's execution.
- The OSCR framework is reusable as similar projects can use the same risk analysis and threat classification.

5.4 Summary

In this chapter, we introduced the OSCR framework for the management of the security and compliance risks of outsourced IT projects. It is designed to meet all identified requirements (previously discussed in Chapter 4) and to overcome any weaknesses in existing ISMS standards and frameworks. Risks associated with all parties involved in the project execution are analysed and managed in a systematic way. It is a structured approach, which uses project phases to manage and control project security risks. The framework is flexible as it follows the PDCA model, which allows the project teams involved in managing security risks to monitor and evaluate security controls continuously, and implement any improvements or changes. Simplicity and ease of use are other features of the OSCR framework as it utilises project phases for the management of security risks, which allows the separate management of security risks during each phase. The OSCR framework is independent from different constraints such as project size or type as it is an asset-based approach. The risks analysis and threat classification of the current project can be applied to new projects that have similarities, making reusability another feature of the OSCR framework.

In the following chapters, the OSCR framework will be evaluated. The evaluation will include a real case study, and also a focus group to provide independent validation evidence.

Chapter 6 Expert Evaluation

As presented in Chapter 5, we have developed the OSCR framework for managing the security and compliance risks of outsourced IT projects. In this chapter we present our first method (experts' evaluation) for evaluating the OSCR framework. It was difficult to find one evaluation method that achieves all the evaluation objectives. Several factors such as cost, time, participants' availability, and IT projects' suitability impose different constraints or limitations on each evaluation method.

6.1 Introduction

The first evaluation method that we used was a focus group and questionnaire. The focus group is a powerful qualitative method that can be used to stimulate and explore participants' experiences, ideas, opinions and attitudes towards the topic under investigation. It relies on interactions between participants to generate rich and detailed data while they discuss the topic with each other and with the researcher. Such dynamic interactions can provide a powerful technique for data generation, especially when existing knowledge about the topic under investigation is not enough, or when the topic is very complex and includes many variables [164, 165].

A focus group has many advantages over other research methods. The three most important advantages that make the focus group a good choice compared with other research methods are exploration and discovery, context and depth, and interpretation. The interactions and discussions with the topic context allow the researcher to collect rich and detailed data, which can be interpreted to form valid evidence about the research topic [166]. Thus, a focus group has the potential to reveal clear opinions about the OSCR framework. Because of these advantages, we decided to employ a focus group for evaluating the OSCR framework and we enhanced it with an online questionnaire.

Our focus group evaluation method was designed to evaluate the usefulness and coverage of each phase and its security units, as well as evaluating the general architecture of the OSCR framework. The aim of this evaluation was to draw ideas and recommendations from relevant people involved in outsourcing. Those people are believed to contribute to improving the OSCR framework by identifying potential weaknesses that it might have or by providing recommendations that help to improve the OSCR framework. The members of the focus group were from a government IT agent in the Middle East that had outsourced more than one hundred IT projects between 2010 and 2017. A variety of projects, including small and large, mission-critical, software and hardware projects, have been executed through different local and international providers. This agent is mature in terms of its security management practices and it follows leading ISMSs such as the ISO 2700x family and SABSA. It also has a Research and Development (R&D) centre and a Project Management Office (PMO) that follows Project Management Institute (PMI) standards. For these reasons, it was decided to recruit experts from this agent and to conduct the focus group at its premises. This provided a convenient way for participants and the researcher to take part in this evaluation and to communicate and discuss their ideas and recommendations without constraints such as time zones or focus group arrangement expenses (e.g. hotels or transport).

The remainder of this chapter is structured as follows: the evaluation objectives and scope are presented in Sections 6.2 and 6.3 respectively. The evaluation hypotheses are stated in Section 6.4. In Section 6.5, the evaluation methodology is explained. We describe the questionnaire design, participants' selection and evaluation procedure in Sections 6.6, 6.7 and 6.8 respectively. In Section 6.9, we present the evaluation results. We analyse the results in Section 6.10. In Section 6.11, a summary of this chapter is provided.

6.2 Evaluation Objectives

The focus group evaluation and the questionnaire were designed to achieve specific objectives. The following lists the general objectives of this evaluation:

1. Identify potential weaknesses that may affect the ability of the OSCR framework to manage the security and compliance risks of outsourced IT projects effectively.
2. Gather recommendations from expert people in outsourcing that could be used to improve the OSCR framework.
3. Evaluate the general architecture of the OSCR framework, including the outsourcing threat classification approach that has been designed for the outsourcing context.

6.3 Evaluation Scope

The scope of the evaluation using the focus group and questionnaire covers different aspects of the OSCR framework such as:

1. Achievement of promising features of the OSCR framework such as simplicity and ease of use.
2. Usefulness of utilising project phases and units in managing the security and compliance risks of outsourced IT projects.
3. Flexibility of the OSCR framework as it utilises the Plan-Do-Check-Act (PDCA) model in managing the security and compliance risks in the outsourcing context.
4. The framework units' coverage of security aspects that need to be taken into consideration in the outsourcing context.
5. Achievement of a systematic and comprehensive methodology for managing the security and compliance risks of outsourced IT projects using the OSCR framework.
6. Effectiveness of the outsourcing threat classification approach for identifying security threats in the outsourcing context.
7. The ability of the OSCR framework to be applied to any project as it is independent from different constraints such as project size, cost or duration.

6.4 Evaluation Hypotheses

Six hypotheses were developed and tested in the evaluation:

1. The OSCR framework is understandable, simple and easy to use [H1].
2. Utilising project phases for managing security and compliance risks is useful in the outsourcing context [H2].
3. The PDCA model improves the flexibility of security and compliance management in the outsourcing context [H3].
4. The OSCR framework provides a systematic and comprehensive methodology for managing the security and compliance risks of outsourced IT projects [H4].
5. Using the outsourcing threat classification approach provides an effective and useful way for identifying security threats in the outsourcing context [H5].
6. The OSCR framework can be generalised and applied to any project as it is independent from different constraints such as project size or cost [H6].

6.5 Evaluation Methodology

The following points summarise the methodology that has been used to conduct this evaluation:

1. Selecting an appropriate agent who has long experience in IT outsourcing, security and compliance risk management.
2. Recruiting appropriate people who meet specific criteria (presented in Section 6.7). These criteria were used to select potential participants including program managers, project managers, PMO officers, security and project team members, and architecture and application development teams from both sides: the client and the provider.
3. Conducting a series of workshops that present the OSCR framework to each group, for example a program managers' workshop, a project

managers' workshop, and so on. Other workshops were conducted for undefined groups such as application and security management teams.

4. Discussing with the attendees their comments and clarifying for them the OSCR framework features. Their recommendations were discussed and considered as well as their criticisms.
5. At the end of each workshop, the attendees were invited to evaluate the OSCR framework and to provide their recommendations in order to improve the OSCR framework, using the online questionnaire.

6.6 Questionnaire Design

The evaluation data of the OSCR framework were collected using an online questionnaire, in addition to the focus group data. The online questionnaire provides a convenient way of collecting data for the researcher and it allows the participants to provide their feedback without time pressures or any other influence such as job role or colleagues' opinions. To encourage the participants to take part in this evaluation, and to save their time, most of the questionnaire questions were guided. However, after each guided question, a space for comments was provided in case the participant wished to add a comment, criticism or recommendation. Several studies have shown that odd numbers of choices could be used as a dumping ground when participants are not sure about their answers or when they want to choose a legitimate answer that is socially desirable [167]. For this reason, the choices of answers were designed carefully. Odd numbers of choices were avoided. This could help to avoid random selection and encourage the participants to think carefully before choosing their appropriate answer. To reduce any influence of bias, such as job role or colleagues' opinions, and to achieve anonymity, the evaluation was completed online and providing names was optional. The evaluation questions were categorised into two groups. The first group concentrated on evaluating the OSCR framework phases and their units. The second group focused on evaluating the general architecture of the OSCR framework.

6.7 Participant Selection

Participation in the workshops and the evaluation was entirely voluntary. However, the invitation was only sent to participants who met specific criteria, as listed below:

1. The participant should have relevant experience in IT projects and related areas such as security and applications development.
2. Participants should have industrial experience in outsourcing IT projects.
3. Participants have experience in a range of IT projects such as small, large, mission-critical and application development projects.
4. Participant's role is program manager, project manager, project team member, PMO officer, security specialist, IT architect, or applications developer.

6.8 Evaluation Procedure

Six groups were identified before conducting the workshops: program managers (client side), project managers (client side), project managers (provider side), project team members (both sides), PMO officers (client side), and security, architecture, and applications team members (both sides). Categorising the attendees into these groups was intended to provide an environment where the participants shared almost the same levels of knowledge, issues and concerns. The other reason for this categorisation was to reduce influence or bias that could result from the participants' job roles, such as the influence of program managers on their project managers or the influence of project managers on their project team members. The last group was for independent participants, who have a wider view as they work on the organisation or provider level rather than at the project level. They have different backgrounds such as application development, security policies and compliance management.

Six focus group workshops were conducted based on the attendees' groups. It was planned that each workshop would be attended by 6-10 participants and last between 60 and 90 minutes. The material was prepared and the questions were determined for the focus groups. To help monitor the recording and other equipment (e.g. projector, PC, etc.), and to arrange refreshments, a moderator was arranged. The location for the focus group workshops was based on the building where the majority of the outsourced IT projects were executed. The invitation was then sent to potential participants with the timetables and location for the workshops.

At each workshop, the researcher welcomed the participants and explained the objectives of the workshop. The participants were told that the information would be confidential and that their anonymity would be maintained as the researcher had signed a Non-Disclosure Agreement (NDA). The researcher then presented the OSCR framework and explained its phases, units and features. During the presentation, the attendees could ask for any clarification. When the researcher had completed the presentation, an open discussion was provided to draw out the attendees' comments, criticisms, suggestions or recommendations. All workshops were recorded in order to allow the researcher to analyse the data carefully. At the end of each workshop, all of the attendees were invited to provide their feedback using the online questionnaire. The workshops were attended by 45 participants. Although the evaluation link was sent to all of the participants by email, no pressure was placed on the attendees to complete it. Despite the lack of pressure, we still received 30 responses. As the researcher has signed an NDA, the exact attendees' comments, criticisms, suggestions or recommendations will not be provided. Instead, a summary of the exact scripts will be presented and discussed in this chapter. This will help to overcome the limitation introduced by signing the NDA.

6.9 Evaluation Results

In this section we present the evaluation results. The IBM SPSS statistics 24 tool was used to analyse the results.

6.9.1 Descriptive statistics

A total of 30 participants responded to the questionnaire. As can be seen from Table 6.1, the organisational distribution shows that the highest number of participants belonged to the client 22 (73.3%), while participants from all the providers were 8 (26.7%).

Table 6.1: Participants' Distribution by Organisation

	Frequency	Percent	Cumulative Percent
Client	22	73.3	73.3
Providers	8	26.7	100.0
Total	30	100.0	

In terms of role, as presented in Table 6.2, most of the people (12, 40.0%), who participated in the study were project managers, whereas the smallest participant category was program managers (4, 13.3%).

Table 6.2: Participants' Distribution by Role

	Frequency	Percent	Cumulative Percent
Program Manager	4	13.3	13.3
Project Manager	12	40.0	53.3
Project Team Member	9	30.0	83.3
Other	5	16.7	100.0
Total	30	100.0	

With regard to qualifications, as shown in Table 6.3, the highest percentage (53.3%) of the participants had a Bachelor degree (n=16). There was only one participant with a Diploma, and similarly another with a PhD.

Table 6.3: Participants' Distribution by Qualification

	Frequency	Percent	Cumulative Percent
Diploma	1	3.3	3.3
Bachelor	16	53.3	56.7
Master	12	40.0	96.7
PhD	1	3.3	100.0
Total	30	100.0	

In terms of work experience, the majority of participants had either more than 10 years' or 7-10 years' experience in IT outsourcing, representing 66.6% in total. Only 13.3% had between 1 and 3 years of work experience in outsourced IT projects. Table 6.4 shows the participants' distribution based on their experience.

Table 6.4: Participants' Distribution by Experience

	Frequency	Percent	Cumulative Percent
1-3 years	4	13.3	13.3
4-6 years	6	20.0	33.3
7-10 years	10	33.3	66.7
more	10	33.3	100.0
Total	30	100.0	

The participants were asked about the current security framework or standard that they used for managing the security risks of outsourced IT projects. The vast majority of the study population did not use any (16, 53.3%). Table 6.5 shows the participants' distribution based on the ISMS they used.

Table 6.5: Participants' Distribution by ISMS Used

	Frequency	Percent	Cumulative Percent
ISO 2700X	8	26.7	26.7
SABSA	4	13.3	40.0
None	16	53.3	93.3
Other	2	6.7	100.0
Total	30	100.0	

6.9.2 Framework Phases and Units Evaluation

This part of the evaluation was designed to evaluate the usefulness (in terms of cost effectiveness, time efficiency and ease of use) of each phase units of the OSCR framework, as well as the coverage of the security aspects of this phase that need to be taken into consideration when managing the security and compliance risks of outsourced IT projects. For the usefulness of the units of each phase, we have used a Likert-type scale using four ranks [167, 168] (not useful, somewhat useful, useful, and very useful). 'Not useful' means that the majority of the units of the phase are unlikely to add any value in terms of managing the security and compliance risks of outsourced IT projects, whereas 'somewhat useful' means that some of the units of the phase are unlikely to add value. 'Useful' means that only a few units of the phase are unlikely to add value. 'Very useful' means that all units of the phase are likely to add value when managing outsourcing security and compliance risks. Although we avoided having an odd number of options for the answers, in order to reduce the use of the middle option as a dumping ground, this introduced potential bias towards the positive options (somewhat useful, useful, and very useful). However, the participants could still choose the negative option (not useful). For the coverage of the security aspects for each phase, we provided four options and the participants could choose one or more of the options. The questionnaire is presented in Appendix A.

6.9.2.1 Initiating Phase Evaluation

The evaluation of the usefulness of the initiating phase, as presented in Table 6.6, shows that 36.7% of the participants voted it as being "very useful", and 53.3% of the participants regarded it as "useful" in terms of managing the security risks of outsourced IT projects. The "somewhat useful" option gained 6.7% of the votes, whereas the "not useful" option has only 3.3% of the participants' votes.

Table 6.6: Initiating Phase Units' Usefulness

	Frequency	Percent	Cumulative Percent
Very useful	11	36.7	36.7
Useful	16	53.3	90.0
Somewhat useful	2	6.7	96.7
Not useful	1	3.3	100.0
Total	30	100.0	

In the evaluation of the coverage of security aspects for the initiating phase, 38.7% of participants thought that these units covered all of the required security aspects. 48.4% of participants indicated that the units covered most of the required security aspects, while the option "misses required security units" was chosen by 6.5% of the participants. The same percentage (6.5%) of the participants' votes went to the option saying that the initiating phase covered unnecessary units. Table 6.7 shows the distribution of the participants across the options provided for this question. It should be noted that the participants could choose more than one option.

Table 6.7: Initiating Phase Coverage

		Responses		Percent of
		N	Percent	Cases
Initiating Phase Coverage	Covers all required security aspects in this phase	12	38.7%	40.0%
	Covers most of the required security aspects in this phase	15	48.4%	50.0%
	Misses required units	2	6.5%	6.7%
	Covers unnecessary units	2	6.5%	6.7%
Total		31	100.0%	103.3%

6.9.2.2 Initiating Phase Comments and Recommendations

In this section, we discuss the participants' comments and recommendations provided during the workshops or through the online questionnaire. Each

comment or recommendation will be stated and the response and the action taken will be provided.

- **Recommendation 1**: It was recommended by a participant to keep the identification of potential security risks at an abstract level to minimise costs.

  Response: The risk identification task is vital in order to have risk visibility at an early stage when correction costs are minimal. We see that the more detailed the identification of potential security risks is, the more risk visibility is controlled and mitigated. The level of potential security risks identification, whether an abstract level or not, depends on different factors such as the organisation's resources and the project's requirements.

  Action: No change to the OSCR framework.
- **Recommendation 2**: One participant suggested moving the potential security risks unit to the planning phase to minimise the time and cost required for this process.

  Response: The aim of this unit is to identify potential security risks that might take place while executing the project. This allows decision makers to take the right decision over whether to outsource or not before contracting with the provider. If we move this unit to the planning phase, the organisation may enter a contract without realising the security risks associated with this contract.

  Action: No change to the OSCR framework.
- **Recommendation 3**: Another participant suggested adding an infrastructure/asset unit at this phase. This is to identify security risks at a network level and the required implementations such as firewall, protocols etc.

  Response: Although this suggestion seems to be beneficial, it will be difficult to implement it at this phase using a new unit as there is no project yet. Additionally, the OSCR framework has an assets unit at the planning phase, which includes network and infrastructure assets.

Action: No change to the OSCR framework.

- **Recommendation 4**: The last suggestion was to add a new unit for implementing security mitigations that can mitigate the identified potential security risks before outsourcing.

  Response: We see this suggestion as valid and it does not conflict with any unit in the other phases.

  Action: the OSCR framework was updated to accommodate this suggestion.

6.9.2.3 Planning Phase

The usefulness evaluation of the planning phase units was conducted in a similar way to that of the initiating phase evaluation. In Table 6.8, we can see that 43.3% of the participants voted in favour of the "very useful" option. 46.7% of the participants said that the planning phase units were useful for managing the security and compliance risks of outsourced IT projects. 6.7% of the total participants' votes went to the option "somewhat useful", while the "not useful" option was selected by only 3.3% of the participants.

Table 6.8: Planning Phase Usefulness

	Frequency	Percent	Cumulative Percent
Very useful	13	43.3	43.3
Useful	14	46.7	90.0
Somewhat useful	2	6.7	96.7
Not useful	1	3.3	100.0
Total	30	100.0	

Having evaluated the usefulness of the planning phase units, the participants evaluated the coverage of the security aspects in this phase. In Table 6.9, we see that 45.2% of the participants were in favour of the option that says that the planning phase covers all the required security aspects. The option "covers most security aspects in this phase" was chosen by 51.6% of the participants, whereas

the option “covers unnecessary units” received 3.2% of the participants’ votes. The option “misses some required units” was not selected by any participants.

Table 6.9: Planning Phase Coverage

		Responses		Percent of
		N	Percent	Cases
Planning Phase Coverage	Covers all required security aspects in this phase	14	45.2%	46.7%
	Covers most of the required security aspects in this phase	16	51.6%	53.3%
	Covers unnecessary units	1	3.2%	3.3%
Total		31	100.0%	103.3%

6.9.2.4 Planning Phase Comments and Recommendations

- **Comment 1:** A comment from a participant says that these units present a methodological approach towards having correct risk identification and understanding, which consequently enables proper risk planning.

  Response: This comment exactly complies with the OSCR framework goals. The identification and assessment of security risks and security controls should be carried out early in the life cycle of the project by the two parties, the outsourced project provider and the client. This will allow proper handling of all risks at the early stages of the project life cycle where corrections can usually be made at minimum costs.

  Action: No change to the OSCR framework.
- **Recommendation 1:** A human unit was suggested by a participant. According to this suggestion, a new human unit should be added to the OSCR framework to identify the number and roles of key resources involved in executing the project. Humans are considered to be a risk and the OSCR framework should identify their security risks in the project.

- **Response:** Taking this suggestion into consideration, we found that human resources are part of the project assets. The OSCR framework has a unit for project assets but does not take the human element into consideration.
- **Action:** The OSCR framework was updated to accommodate this recommendation**.**
- **Recommendation 2:** Another suggestion says that the threat classification unit, the risk assessment unit, and the risk repository unit should be integrated together to form one unit called the risk assessment unit.

  Response: The threat classification unit represents the method that we developed for the outsourcing context. The output of this unit is a list of threats based on the project assets that might take place while executing the project. The risk repository unit is intended to contain a list of all the active risks that have been assessed through the risk assessment unit. Active risks are accessed and monitored by project teams, such as project steering committees and PMO officers, even if they are not involved in the risk assessment process. Although integrating all the three units is feasible, we do not see any added value from doing so. In contrast, keeping those units as separate units provides a better understanding for those units, especially during the first use the OSCR framework and it does not provide irrelevant information that might not be required by different teams.

  Action: No change to the OSCR framework.
- **Recommendation 3:** The last suggestion recommends moving the assets unit to the next phase. The rationale behind this recommendation is the fact that during the planning phase, assets might not represent the whole project assets and new ones might be added later, based on project requirements or security control changes.

  Response: The assets unit is vital for identifying security risks and it cannot be moved to the next phase. However, the OSCR framework is

built on the PDCA model, which facilitates the addition of any new project assets and which includes all of the required risk identification and assessment.

Action: No change to the OSCR framework.

6.9.2.5 Executing Phase

From Table 6.10, we see that 36.7% of the participants thought that the executing phase was very useful, while 56.7% of the participants saw it as being useful. The "somewhat useful" and "not useful" options were selected by 3.3% of the participants each.

Table 6.10: Executing Phase Units' Usefulness

	Frequency	Percent	Cumulative Percent
Very useful	11	36.7	36.7
Useful	17	56.7	93.3
Somewhat useful	1	3.3	96.7
Not useful	1	3.3	100.0
Total	30	100.0	

In Table 6.11, the evaluation of the coverage of security aspects for the executing phase shows that 40% of the participants considered that the units in this phase covered all the required security aspects. 50% of the votes went to the option "covers most of the required security aspects in this phase". 6.7% of the participants were in favour of the option "misses required units", while the option "covers unnecessary units" was selected by 3.3% of the participants.

Table 6.11: Executing Phase Coverage

		Responses		Percent of
		N	Percent	Cases
Executing Phase Coverage	Covers all required security aspects in this phase	12	40.0%	40.0%
	Covers most of the required security aspects in this phase	15	50.0%	50.0%
	Misses required units	2	6.7%	6.7%
	Covers unnecessary units	1	3.3%	3.3%
Total		30	100.0%	100.0%

6.9.2.6 Executing Phase Comments and Recommendations

- **Recommendation 1:** Two participants suggested moving the performance unit and security issues unit to the next phase as the attention at this phase will be on the project's functional requirements.
  Response: The executing phase is the stage where the deliverables are gradually coming into existence through the project's execution timeline. As the focus, during this phase, is traditionally on the functional requirements of the project, the security requirements might be overlooked. Therefore, the executing phase units try to prevent this issue from happening, and security risks are considered as part of every deliverable through the executing phase.
  Action: No change to the OSCR framework.
- **Recommendation 2:** There was also a recommendation suggesting that a project unit be added, which is currently in the initiating phase, to the executing phase specifically and to all other phases in general.
  Response: The project unit is designed to handle (create, update) essential project data such as project ID, name, code etc. The essential data needs to be created once when initiating the project and it rarely needs to be updated during the upcoming phases. Adding the project units to all or some of the other phases of the OSCR framework does

not have any added value and conflicts with the original aim of the project unit.

Action: No change to the OSCR framework.

6.9.2.7 Monitoring and Controlling Phase

In Table 6.12, the evaluation of the usefulness of the monitoring and controlling phase units shows that 33.3% of the participants voted for the option "very useful". 50% of the votes went to the option "useful" while the option "somewhat useful" gained 13.3% of the total votes. The last option "not useful" was selected by 3.3% of the participants.

Table 6.12: Monitoring and Controlling Phase Units' Usefulness

	Frequency	Percent	Cumulative Percent
Very useful	10	33.3	33.3
Useful	15	50.0	83.3
Somewhat useful	4	13.3	96.7
Not useful	1	3.3	100.0
Total	30	100.0	

With relation to the coverage of security aspects in the monitoring and controlling phase, 40% of the participants thought that these aspects were covered in this phase. The second option, "covers most of the required security aspects in this phase", was selected by 46.3% of the participants. 13.3% of the participants thought that the monitoring and controlling phase was missing some of the required units, but no-one thought that it covered unnecessary units. Table 6.13 shows the participants' distribution across the options provided for this question.

Table 6.13: Monitoring and Controlling Phase Coverage

		Responses		Percent of
		N	Percent	Cases
Monitoring and Controlling Coverage	Covers all required security aspects in this phase	12	40.0%	40.0%
	Covers most of the required security aspects in this phase	14	46.7%	46.7%
	Misses required units	4	13.3%	13.3%
Total		30	100.0%	100.0%

6.9.2.8 Monitoring and Controlling Phase Comments and Recommendations

- **Recommendation 1:** Some participants recommended merging the units of this phase with the previous phase units.

  Response: The monitoring and controlling phase aims to review the execution performance reports, and to assess whether there is any need for improvement. Moreover, the project steering committee supports the project manager in resolving security issues that require intervention. Security change requests and security deliverables are reviewed and approved during this phase too. Therefore, this phase should be a separate phase to guarantee that the project teams who execute the project do not act as decision makers, approving their own performance reports, security change requests or security deliverables.

  Action: No change to the OSCR framework.
- **Recommendation 2:** Another comment was raised about the performance unit. The participant sees that this unit could add extra cost and time to the project.

  Response: This comment might be true, however, adding a little extra cost and time is better than delivering a project with security issues and threats that might lead to major security incidents, which could cost the organisation a great deal of effort and costs.

Action: No change to the OSCR framework.

6.9.2.9 Closing Phase

At the end of this part of the evaluation, the participants evaluated the usefulness of the closing phase units. 40% of the participants chose the option "very useful". The second option, "useful", was selected by 40% of the participants. The "somewhat useful" option was favoured by 16.7% of the participants. The last option, "not useful", gathered 3.3% of the participants' votes. Table 6.14 shows the distribution of the participants across the options provided for this question.

Table 6.14: Closing Phase Units' Usefulness

	Frequency	Percent	Cumulative Percent
Very useful	12	40.0	40.0
Useful	12	40.0	80.0
Somewhat useful	5	16.7	96.7
Not useful	1	3.3	100.0
Total	30	100.0	

In terms of the closing phase's coverage, 38.7% of the participants considered that the closing phase covered all the required security aspects. 51.6% of the participants evaluated this phase as covering most of the security aspects that need to be considered when managing the security and compliance risks of outsourced IT projects. The third option, "misses required units", was chosen by 3.2% of the participants, whereas the fourth option gained 6.5% of the participants' votes. Table 6.15 shows the distribution of the participants votes across the options provided for selection for this question.

Table 6.15: Closing Phase Coverage

		Responses		Percent of
		N	Percent	Cases
Closing Phase Coverage	Covers all required security aspects in this phase	12	38.7%	40.0%
	Covers most of the required security aspects in this phase	16	51.6%	53.3%
	Misses required units	1	3.2%	3.3%
	Covers unnecessary units	2	6.5%	6.7%
Total		31	100.0%	103.3%

6.9.2.10 Closing Phase Comments and Recommendations

- **Recommendation 1:** The first recommendation in this phase was to move the auditing unit to the previous phase; without achieving compliance, we cannot move to project closure.

  Response: This recommendation is valid as compliance management should be a continuous activity rather than one process.

  Action: the OSCR framework has been updated to reflect this recommendation. First, at the planning phase, we introduced a new unit called the compliance requirements unit in order to plan what will be audited to demonstrate security compliance. Second, the auditing unit was moved from the closing phase to the monitoring and controlling phase and renamed the compliance auditing unit, to be used by the project steering committee to assess the level of compliance with the requirements during project execution. Finally, at the closing phase, we substituted the auditing unit with the compliance acceptance unit in order to accept or reject the compliance based on the project steering committee's assessment.
- **Recommendation 2:** Another recommendation was adding a new test unit for testing the security requirements and all security plans and controls.

Response: Carrying out a comprehensive test at the closing phase might require a great deal of resources and efforts and might lead to a project delay. If the compliance and auditing are carried out correctly in the previous phases, compliance acceptance at this phase would be sufficient.

- **Action:** No change to the OSCR framework.

6.9.3 Framework General Architecture Evaluation

This section of the evaluation was designed to evaluate the general architecture of the OSCR framework. The evaluation questions will be stated, followed by their relevant results.

1. *The main architecture of the OSCR framework is:*
   - □ *Understandable.*
   - □ *Simple and easy to use.*
   - □ *Difficult.*
   - □ *Requires some improvements (please comment):*

The evaluation result for this question, as presented in Table 6.16, shows that 33.3% of the participants said that the OSCR framework is understandable. 51.3% of the participants chose the option "simple and easy to use". The option that describes the OSCR framework as difficult was not selected by any participants, whereas 15.4% chose the last option, which says that the OSCR framework requires some improvements. It should be noted that the participants could select more than one option.

Table 6.16: Framework General Architecture Evaluation

		Responses		Percent of
		N	Percent	Cases
Framework General Architecture	Understandable	13	33.3%	43.3%
	Simple and easy to use	20	51.3%	66.7%
	Requires some improvements	6	15.4%	20.0%
Total		39	100.0%	130.0%

2. *Utilising project phases in managing security risks of outsourced IT projects is:*

   O Not useful O Somewhat Useful O Useful O Very useful

The respondents' answers to this question show that 46.7% agreed that utilising project phases is very useful, while 43.3% selected the option "useful". The "somewhat useful" option was chosen by 6.7% of the participants, while the "not useful" option was selected by 3.3% of the participants. Table 6.17 shows the distribution of the participants' evaluations across the options provided for selection.

Table 6.17: Utilising project phases

	Frequency	Percent	Cumulative Percent
Very useful	14	46.7	46.7
Useful	13	43.3	90.0
Somewhat useful	2	6.7	96.7
Not useful	1	3.3	100.0
Total	30	100.0	

3. *To what extent do you agree with the statement that adopting the Plan-Do-Check-Act (PDCA) model in managing security risks of outsourced IT projects improves the framework flexibility?*

   O Disagree O Neutral O Somewhat Agree O Agree

50% of the participants agreed with the statement, while 26.7% somewhat agreed. The "neutral" option was selected by 20% of the participants, whereas 3.3% disagreed. Table 6.18 shows the distribution of the participants' evaluations across the options provided for selection.

Table 6.18: PDCA Model Statement

	Frequency	Percent	Cumulative Percent
Agree	15	50.0	50.0
Somewhat Agree	8	26.7	76.7
Neutral	6	20.0	96.7
Disagree	1	3.3	100.0
Total	30	100.0	

4. *Do you agree with the statement that the OSCR framework provides a systematic and comprehensive approach for managing the security and compliance risks of outsourced IT projects?*

   O Disagree O Neutral O Somewhat Agree O Agree

73.3% of the participants agreed with this statement, whereas 10% of the participants somewhat agreed. 13.3% chose the "neutral" option, and 3% disagreed with this statement. Table 6.19 shows the distribution of the participants' evaluation across the options provided for selection.

Table 6.19: Systematic and Comprehensive Statement

	Frequency	Percent	Cumulative Percent
Agree	22	73.3	73.3
Somewhat Agree	3	10.0	83.3
Neutral	4	13.3	96.7
Disagree	1	3.3	100.0
Total	30	100.0	

5. *The outsourcing threat classification approach provides an effective and useful way for identifying security threats in outsourcing context.*

   O Disagree O Neutral O Somewhat Agree O Agree

76.7% of the participants agreed with this statement while 6.7% somewhat agreed. 13.3% of the participants chose the "neutral" option, whereas 3.3% disagreed with this statement. Table 6.20 shows the distribution of the participants' evaluations across the options provided for selection.

Table 6.20: Threat Classification Approach Statement

	Frequency	Percent	Cumulative Percent
Agree	23	76.7	76.7
Somewhat Agree	2	6.7	83.3
Neutral	4	13.3	96.7
Disagree	1	3.3	100.0
Total	30	100.0	

6. *To what extent do you agree that the OSCR framework can be applied to any outsourced IT project as it is independent from different constraints such as project size, cost, or any other constraints?*
   O Disagree O Neutral O Somewhat Agree O Agree

The evaluation result for this question shows that 70% of the participants agreed with this statement. 13.3% of the participants chose the option "somewhat agree", whereas 13.3% of the participants chose the "neutral" option. 3.3% of the participants disagreed with this statement. Table 6.21 shows the distribution of the participants' evaluations across the options provided for selection.

Table 6.21: Framework Generality

	Frequency	Percent	Cumulative Percent
Agree	21	70.0	70.0
Somewhat Agree	4	13.3	83.3
Neutral	4	13.3	96.7
Disagree	1	3.3	100.0
Total	30	100.0	

6.10 Evaluation Analysis

In order to analyse the results accurately in a quantitative way, a Likert scale was used and scaled from 1 to 4 as shown in Table 6.22 and Table 6.23. The weighted mean *(M)* and standard deviation (*SD*) were then used. The weighted mean *(M)* was used to identify the overall results for the usefulness of each phase units as well as the overall results for the general architecture of the framework.

The standard deviation (*SD*) was used to know how the participants' results differed from the mean value.

Table 6.22: Weighted Mean (Very useful, Useful, Somewhat useful, Not useful)

Level	Weight	Weighted Mean
Very useful	1	From 1 to 1.74
Useful	2	From 1.75 to 2.49
Somewhat Useful	3	From 2.50 to 3.24
Not useful	4	From 3.25 to 4

Table 6.23: Weighted Mean (Agree, Somewhat Agree, Neutral, Disagree)

Level	Weight	Weighted Mean
Agree	1	From 1 to 1.74
Somewhat Agree	2	From 1.75 to 2.49
Neutral	3	From 2.50 to 3.24
Disagree	4	From 3.25 to 4

Table 6.24 presents a summary of the evaluation results, weighted mean, standard deviation and overall results. It illustrates that the participants' overall result was "useful" when they were evaluating the units' usefulness for the initiating, monitoring and controlling and closing phases. When they were evaluating the units' usefulness for the planning and executing phases, their overall result was "very useful".

As can be seen from Table 6.24, the majority of the participants chose either the option "very useful" or "useful" for all the framework phases. Only one participant chose the option "not useful". Based on their feedback, the OSCR framework needs to be incorporated with the PMI current processes, or a new knowledge area should be added. Although integrating the OSCR framework with the PMI standard is feasible, it conflicts with our objective to make the framework independent from any existing standard or framework. This will allow any organisation to use the OSCR framework without the need to change their existing security or project management standards.

Table 6.24: Framework Phases and Units Evaluation Summary

Evaluation	Very Useful	Useful	Somehow Useful	Not Useful	Weighted Mean	SD Deviation	Overall Result
	N	N	N	N			
	%	%	%	%			
Initiating Phase Units	11	16	2	1	1.77	0.73	Useful
	36.7	53.3	6.7	3.3			
Planning Phase Units	13	14	2	1	1.70	0.75	Very Useful
	43.3	46.7	6.7	3.3			
Executing Phase Units	11	17	1	1	1.73	0.69	Very Useful
	36.7	56.7	3.3	3.3			
Monitoring and Controlling Phase Units	10	15	4	1	1.87	0.78	Useful
	33.3	50.0	13.3	3.3			
Closing Phase Units	12	12	5	1	1.83	0.83	Useful
	40.0	40.0	16.7	3.3			

For the evaluation of hypotheses, we will restate each hypothesis and discuss whether it has been accepted or not.

1. *The OSCR framework is understandable, simple and easy to use [H1].*

To test this hypothesis, the participants were asked to evaluate the general architecture of the OSCR framework by choosing the appropriate answers. Four options were provided for selection as presented earlier in Section 6.9.3 Table 6.16. The majority of the participants chose understandable or simple and easy to use (84.6%). This supports that the OSCR framework is understandable, simple and easy to use.

2. *Utilising project phases for managing security and compliance risks is useful in the outsourcing context [H2].*

In order to test this hypothesis, the participants were asked to rate the usefulness of utilising project phases for managing security and compliance risks in the outsourcing context. From Table 6.25, it can be seen that the majority of the participants chose “very useful” and “useful” and the overall result is “very useful”. This result supports that utilising project phases for managing security and compliance risks is useful.

Table 6.25: Utilising project phases – summary

Evaluation	Very Useful	Useful	Somehow Useful	Not Useful	Weighted Mean	SD Deviation	Overall Result
	N	N	N	N			
	%	%	%	%			
H2	14	13	2	1	1.67	0.76	Very Useful
	46.7	43.3	6.7	3.3			

3. *The PDCA model improves the flexibility of security and compliance management in the outsourcing context [H3].*

One of the OSCR framework features is the PDCA model. The framework utilises the Plan-Do-Check-Act (PDCA) model to improve its flexibility to deal with changes in security requirements, controls and plans, which are more often encountered in outsourced IT projects. The participants were asked if they agreed that utilising the PDCA model improved the OSCR framework's flexibility in the outsourcing context. As can be seen in Table 6.26, the "somewhat agree" option was the participants' overall result towards this question. This result supports that adopting the PDCA model makes the OSCR framework more flexible in the outsourcing context.

4. *The OSCR framework provides a systematic and comprehensive methodology for managing the security and compliance risks of outsourced IT projects [H4].*

The majority of the participants chose the options "agree" or "somewhat agree" when they were asked whether they agreed or not with the statement that says the OSCR framework provides a systematic and comprehensive methodology for security management in the outsourcing context. Table 6.26 shows that the participants' overall response was to agree with this statement, which indicates that this hypothesis is supported.

5. *Using the outsourcing threat classification approach provides an effective and useful way of identifying security threats in the outsourcing context [H5].*

To test this hypothesis, the participants were asked if they agreed or not that using the proposed threat classification approach provided an effective and useful way of identifying security threats in the outsourcing context. The results in Table 6.26 show that the participants' overall response was to agree, which indicates that this hypothesis is supported.

6. *The OSCR framework can be generalised and applied to any project as it is independent from different constraints such as project size or cost [H6].*

The OSCR framework was designed to be independent from different constraints such as project size, cost or duration. The participants were asked if they agreed or not with this statement. The participants' overall response was to select "agree", which indicates that this hypothesis is supported.

Table 6.26: Overall Evaluation Summary

Overall Evaluation	Agree	Somewhat Agree	Neutral	Disagree	Weighted Mean	SD Deviation	Overall Result
	N	N	N	N			
	%	%	%	%			
H3	15	8	6	1	1.77	0.90	Somewhat Agree
	50.0	26.7	20	3.3			
H4	22	3	4	1	1.47	0.86	Agree
	73.3	10	13.3	3.3			
H5	23	2	4	1	1.43	0.86	Agree
	76.7	6.7	13.3	3.3			
H6	21	4	4	1	1.50	0.86	Agree
	70	13.3	13.3	3.3			

6.11 Summary

In this chapter, we have presented our evaluation results for the OSCR framework for managing the security and compliance risks of outsourced IT projects. The first method that we used to evaluate the OSCR framework was a focus group, enhanced by a questionnaire. The focus group method has several advantages such as gathering in-depth information, and being able to expand

and clarify questions. The focus groups were conducted with experienced IT agents. Several outsourced IT projects have been executed by local and international providers for this agent.

The evaluation results show that the OSCR framework has achieved reasonable acceptance in the outsourcing context. All the hypotheses were supported by the participants. Several features such as its flexibility, simplicity and ease of use have been acknowledged by the participants. The OSCR framework provides a comprehensive methodology that is capable of providing organisations with the ability to minimise, mitigate or eliminate security risks in the early stages of project execution. It is also acknowledged by the participants that the OSCR framework is strengthened by a robust threat classification approach that improves threat identification in the outsourcing context. Bearing in mind that outsourcing environments are less stable and more systems are integrated together, the OSCR framework is enhanced by the PDCA model, which provides a continuous improvement process to accommodate the changes and improvements required while executing the project.

The participants' recommendations contributed to improving our understanding of different factors that need to be considered when managing the security and compliance risks of outsourced IT projects. The following summarises these factors:

- Outsourcing compliance management is a continuous process that should be carried out throughout the project execution, rather than one process carried out before closing the project.
- Humans should also be considered as a source of security risks and their potential impact should be analysed and controlled.
- Other factors, such as the cost of managing the security and compliance risks of outsourced IT projects, should be considered. A balance between security risk management and cost should be achieved as not all organisations are able to afford costs that might be outside their budget boundaries.

With the consideration of the valuable recommendations from the participants, the OSCR framework has been updated and improved. The recommendations are believed to improve the OSCR framework's ability to manage security and compliance risks in a more effective way in the outsourcing context. The following summarises the updates to the OSCR framework resulted from the participants' recommendations:

- At the initiating phase, a new unit was added for implementing security mitigations, in order to mitigate the identified potential security risks before outsourcing.
- At the planning phase, another unit, called the compliance requirements unit, was added. This provides a role for the organisation/project manager to plan what will be reviewed when auditing the security of the project.
- At the monitoring and controlling phase, the auditing unit was moved from the closing phase and renamed the compliance auditing unit in order to assess the level of compliance with security requirements.
- Finally, at the closing phase, we substituted the auditing unit with the compliance acceptance unit to accept or reject the assessment of the compliance with security requirements.

Although the number of participants is quite small, they represented a good representative sample, as they are experienced in outsourced IT projects and their security and compliance risks.

In the following chapter, the framework is applied to real outsourced IT projects as a case study.

Chapter 7 Case Study Evaluation

In the previous chapter, the OSCR framework for outsourced IT projects was evaluated by experts using a focus group and questionnaire. This chapter represents the empirical case study method that we used to evaluate the OSCR framework. The aim of this case study was to evaluate the novelty of the OSCR framework and to assess its ability to manage the security and compliance risks of IT projects in the outsourcing context effectively. It also aimed to discover potential changes and improvements that could enhance the OSCR framework's performance when outsourcing IT projects. It should be noted that this case study is different from the API/PNR case study we used for illustration in Chapter 5.

7.1 Introduction

Among research methods (e.g. survey, action research, etc.), the case study method was chosen to evaluate the OSCR framework. The case study method offers several benefits [169]. The following highlight some of these benefits:

- Using real outsourced IT projects provides the researcher with a holistic view and a deep understanding of the phenomena as it facilitates the description and explanation of a research problem or situation [170, 171].
- It allows the researcher to investigate the ability of the OSCR framework to manage the security and compliance risks of outsourced IT projects effectively in their real-life context.
- The rich and in-depth data that can be obtained helps the researcher to understand the complexity of the outsourcing context, in which the client, providers and stakeholders interact together during the execution time of the projects.
- The practical knowledge and experience of the participants could help discover potential weaknesses and provide some valuable recommendations, which could contribute to improving the OSCR framework.

Past literature has identified several guidelines for conducting a rigorous case study. In spite of the fact that these guidelines do not guarantee the quality of the case study, they provide the researcher with practical measures for conducting a rigorous case study that aims to provide evidence about the phenomena under investigation from the data being collected. For this reason, the guidelines in [172-174] were taking into consideration when conducting this case study.

The remainder of this chapter is structured as follows: the evaluation objectives and scope are presented in Sections 7.2 and 7.3 respectively. In Section 7.4, the evaluation methodology is explained. We discuss the projects' selection in Section 7.5. We describe the evaluation procedure, evaluation data source, and how to reduce evaluation bias in Sections 7.6, 7.7, and 7.8 respectively. In Section 7.9, we highlight the case study validity and in Section 7.10 we present the evaluation results. Changes to the OSCR framework resulted from all of the evaluation methods used, and these are presented in Section 7.11. We analyse and compare the OSCR framework with the existing ISMS standards and framework in Section 7.12. In Section 7.13, a summary of this chapter is provided.

7.2 Evaluation Objectives

The case study was designed to achieve the following objectives:

1. Assess the ability of the OSCR framework to effectively manage the security and compliance risks of outsourced IT projects.
2. Draw ideas and recommendations from relevant people involved in outsourcing, which can be used to improve the OSCR framework.
3. Discover potential drawbacks and weaknesses that might affect the ability of the OSCR framework to manage the security and compliance risks of outsourced IT projects effectively.

7.3 Evaluation Scope

The scope of the evaluation using a case study covers different aspects of the OSCR framework:

1. The effectiveness of the OSCR framework to manage the security risks of outsourced IT projects compared to the security management standards and frameworks used by the client and providers.
2. The effectiveness of the outsourcing threat classification to identify potential security threats in the outsourcing context.
3. The ability of the OSCR framework to provide a comprehensive methodology for managing security and compliance risks in the outsourcing context.
4. The ability of the OSCR framework to enhance compliance enforcement throughout project execution.
5. The flexibility and ease of use of the OSCR framework to manage the security risks of outsourced IT projects and to be independent from different constraints such as project type, cost or time.

In spite of the fact that the scope of the case study might overlap with the scope of the focus group and questionnaire, which were discussed in the previous chapter, it represents the practical part of the evaluation. Those diverse evaluation methods (focus group, questionnaire, and case study) were used also to provide independent validation evidence.

7.4 Evaluation Methodology

The following steps summarise the methodology that has been used to conduct this case study:

1. Appropriate agents were found who had long experience in IT outsourcing, security and compliance risk management.
2. Researcher signed the Non-Disclosure Agreement (NDA).

3. Outsourced IT projects were selected that met the specific criteria used for selecting potential projects (presented in Section 7.5).
4. An introductory workshop was conducted for all participants. The OSCR framework was explained and discussed in the workshop.
5. Participants who agreed to take part in this case study signed the consent form.
6. Participants were provided with the material and templates (provided in Appendix B), and with the researchers' contact details in case they needed some extra clarifications.
7. The participants applied the OSCR framework to the selected outsourced IT projects.
8. Project data was shared with the researcher at the end of each phase of the OSCR framework.
9. The participants provided the researcher with their overall feedback at the end of the project's execution.

7.5 Project Selection

The selection of the outsourced IT projects that were used as the case study was made following the below criteria:

1. The project execution time should not exceed six months, in order to meet the research's time constraint.
2. The selected projects should be executed by two different providers with diverse security experience and practices.
3. The selected projects should differ in their missions and objectives in order to allow the OSCR framework to be evaluated as far as possible in different security aspects (e.g. hardware, software, network, and so on).
4. The providers should have security experience and there should have been no major security incidents with the client.

7.6 Evaluation Procedure

Based on the selection criteria (Section 7.5), two projects were chosen. Table 7.1 and Table 7.2 provide information about these two projects. The two projects were executed by two different providers for the same client. The participants in the case study worked for an IT agent for the government and local and international providers. Their combined experiences covered a wide range of outsourced IT projects, including mission-critical, software and hardware IT projects of different sizes. The OSCR framework was applied to the two outsourced IT projects from the beginning of the projects' execution until their end.

Table 7.1: Case Study First Project

Provider Type	**Provider Size**	**Provider Main Business**
International	+ 4700 Employees	Air Transport Industry
Project Type	**Project Time**	**Project Cost**
Turn-key solution	6 Months	$ 5000000
Project Description		
The project will automate the border processes at one international airport. Travellers will be able to exit or enter the country using self-service machines. If the system succeeds, it will be deployed at all international airport across the country. The project involved software development, hardware deployment, and integration with the client's relevant applications and ISs.		

Table 7.2: Case Study Second Project

Provider Type	**Provider Size**	**Provider Main Business**
Local	50-100 Employees	Information Technology Solutions
Project Type	**Project Time**	**Project Cost**
Turn-key solution	6 Months	$ 1000000
Project Description		
The project will enable police officers to use a mobile application while they are carrying out their field duties so that they can perform some of their ongoing activities without the need to contact police centres (e.g. information checks about people, cars etc.). The project also involved software development and integration with the client's relevant applications and ISs.		

Following the selection of the two projects for the case study, an invitation was sent to the two project members to attend an introductory workshop. In the workshop, the researcher explained the objectives of the case study and presented the OSCR framework. The participants were told that information would be confidential and that their anonymity would be maintained as the researcher had signed the NDA. The application of the OSCR framework was explained, as well as the templates that were designed for data collection. The participants who agreed to take part in the case study then signed the consent form.

For each project, there was one project owner from the client, one project manager and two project team members from the providers involved in the case study. The project owner oversaw the project execution and facilitated communications with the client's relevant departments (PMO, Finance etc.) The project manager was responsible for the project teams and the execution of the whole project. The project team members were responsible for implementing the project's planned tasks.

Although the start dates for the two projects were almost the same (one week's difference), the OSCR framework was applied to the two projects separately. The two providers were located by the client in two different buildings (client criteria). There was no direct communication between the participants from the two providers. During the implementation of the OSCR framework, the researcher engaged with the participants through different communication methods to clarify any aspects of the OSCR framework. At the end of each phase, the participants shared the project data with the researcher using the templates given to them. The project data were then analysed and processed. If there were any issues with applying the OSCR framework accurately, the researcher resolved the issue with the relevant participants. As the researcher conducted a workshop for all the participants and engaged with the participants during all the project phases through different communication methods, there were no

major issues with the application of the OSCR framework to the projects. The following summarises the case study procedure:

1. At the initiating phase, the OSCR framework was used by the client participants to identify the project's essential data, potential security risks and stakeholders. The data were then shared with the researcher at the end of this phase.
2. At the planning phase, the units of the OSCR framework were used by the client and providers to identify the security requirements and the projects' assets. The outsourcing threat classification approach was then used to identify the security risks associated with executing the projects. The participants then followed the OSCR framework approach to assess the identified security risks and proposed security controls that were believed to avoid or mitigate the impact of the identified security risks. Roles, responsibilities and security plans were identified and reviewed. At the end of the planning phase, the participants shared the project data with the researcher.
3. At the execution phase, the participants put their plans into practice. The OSCR framework units were used to submit the performance reports and to record security issues and security change requests. At the end of this phase, the project data was sent to the researcher.
4. At the monitoring and controlling phase, the OSCR framework was used to review and approve or reject the performance reports. Improvements were proposed and implemented where required. Security issues that needed intervention from the project steering committee were reviewed and resolved. The security Change Requests Unit was used to analyse and approve or reject all received security change requests. The participants at the end of this phase shared the project data with the researcher.
5. At the closing phase, the OSCR framework units were used to document security lessons learned and to accept or reject the security compliance of the two projects. Finally, closure certificates were issued

to the two providers. The project data, along with the overall participants' feedback, were then sent to the researcher.

7.7 Evaluation Data Source

The two projects that have been used as the case study were the data source for this evaluation. The participants were asked to apply the OSCR framework to the two projects and to use the special templates (provided in Appendix B) that have been designed for this purpose during all project phases. Project documents such as Request for Proposal (RFP) and Scope of Work (SOW) were also used to make sure that the security requirements were extracted and implemented according to the client's needs. The researcher and participants used different direct communication methods, such as meetings, emails, or video and voice calls. This allowed the researcher to have reasonable control over the data collection. At the end of the projects' execution, each participant submitted their final feedback on the OSCR framework directly to the researcher. Using separate participant feedback as well as project documents as data sources facilitated data triangulation, which was used to enhance the case study's validity, as will be explained in Section 7.9.

7.8 Reducing Bias

Taking into consideration the fact that by their nature case studies are vulnerable to bias, four sources of bias were identified in this case study: fear of external influence, restrictions, time pressure, and environment changes. The researcher has taken this into account and used the following measures to reduce bias as far as possible:

1. The participants were told that the researcher had signed the client NDA and that all collected data would be confidential and not be shared with their employers or anyone else. Projects' and participants' privacy and anonymity would be maintained. All of the collected data would only be used by the researcher and his supervisor for the purpose

of evaluating the OSCR framework. This ensured that the participants gave their feedback without any external influence (e.g. employer influence).

2. No influence or restrictions were placed on the participants. The OSCR framework was applied to the two projects by the participants only. The researcher conducted the introductory workshop, provided the participants with the material and case study templates, and answered any questions asked by the participants.
3. No time pressure was put on the participants and the OSCR framework was applied to the two projects from the beginning of the projects' execution until their end. The environment was maintained the same, with no changes, during the projects' execution.
4. At the end of the projects' execution, each participant provided their overall feedback separately to avoid any external influence (e.g. job role, colleague influence etc.).
5. All project data were collected using the templates provided to the participants. This allowed the researcher to review and analyse the case study results carefully without any time constraints, which might lead the researcher toward the desired conclusion only.

7.9 Case Study Validity

To enhance the validity of the case study outcomes, the construct validity, internal validity, external validity, and reliability were considered during all case study phases [172].

Construct Validity: deals with operational measures that can be employed to provide a degree of certainty that the case study measures what was intended by the researcher. Construct validity was considered by developing a simplified procedure for the case study, conducting a workshop to explain how to apply the OSCR framework, and providing the participants with all the required material and templates. Using multiple sources of evidence, reviewing the case study

reports by key informants, and maintaining a chain of evidence were strategies employed to ensure construct validity.

Internal Validity: is concerned with how to justify the causal relationships between the case study factors such as time pressure or environment changes. The participants were allowed to apply the OSCR framework from the beginning of the projects' execution until their end. There was no time pressure on them to rush. The two projects were executed without any environment changes. To increase the internal validity, data source triangulation was employed (e.g. collecting data from the participants and from the project documents).

External Validity: is concerned with knowing whether the case study results can be generalised to other cases or not. In spite of the fact that the OSCR framework could not be applied to more than two projects due to several constraints (e.g. the research time, travel cost, security and privacy issues), the case study represented two real outsourced IT projects in their live context. Two different providers applied the OSCR framework to the projects. The type, size and mission of the two projects were different. As a result of this, we suggest that the case study results can be generalised to other cases.

Reliability: is concerned with showing that other investigators can obtain the same case study results if they use the same procedure for the data collection of the project. Our case study results depended on the results obtained from applying the OSCR frameworks to the two outsourced IT projects. Other researchers who familiarise themselves with the OSCR framework and follow the same procedure for data collection and analysis can replicate the case study results.

7.10 Case Study Results

In this section, we will present and discuss the participants' feedback, issues, and their suggestions and recommendations to improve the OSCR framework. The general evaluation questions will be stated and followed by the participants'

responses. Project-specific data will not be discussed due to confidentiality issues and the need to maintain privacy and anonymity (NDA obligations).

1. *In comparison with the current security standard or framework (e.g. ISO 27000x, SABSA) that you use, how do you rate the* OSCR *framework?*
    - *Provides better management for security risks of outsourced IT projects in all phases.*
    - *Provides better management for security risks in some phases. (Please comment)……..*
    - *Same as the current security framework or standard that you use.*
    - *Provides lower management for security risks of outsourced IT projects.*

In Table 7.3, the evaluation result for this question shows that 62.5% of the participants say that the OSCR framework provides better management for the security risks of outsourced IT projects in all phases. The option that says the OSCR framework provides better management for the security risks of outsourced IT projects in some phases was chosen by 37.5% of the participants. The last two options were not selected by any of the participants.

Table 7.3: Participants Distribution

	Frequency	Percent	Cumulative Percent
Provides better management for security risks of outsourced IT projects in all phases	5	62.5	62.5
Provides better management for security risks in some phases	3	37.5	100.0
Total	8	100.0	

In Table 7.4, the majority of the providers' and half of the client's participants acknowledged that the OSCR framework provides better management for the security risks of outsourced IT projects in all phases. The remaining half of the

client's participants said that it provides better management for security risks of outsourced IT projects in some phases (specifically, the initiating, planning, and monitoring and controlling phases).

Table 7.4: Participants' Distribution by Organisation

			Organisation		
			Client	Provider	Total
Q1	Provides better management for security risks of outsourced IT projects in all phases	Count	1	4	5
		% within Q1	20.0%	80.0%	100.0%
		% within Organisation	50.0%	66.7%	62.5%
		% of Total	12.5%	50.0%	62.5%
	Provides better management for security risks in some phases	Count	1	2	3
		% within Q1	33.3%	66.7%	100.0%
		% within Organisation	50.0%	33.3%	37.5%
		% of Total	12.5%	25.0%	37.5%
Total		Count	2	6	8
		% within Q1	25.0%	75.0%	100.0%
		% within Organisation	100.0%	100.0%	100.0%
		% of Total	25.0%	75.0%	100.0%

2. *What are the issues that you think exist in the* OSCR *framework?*

Based on the participants' responses, the following represent the issues existing in the OSCR framework:

- **Issue 1:** when outsourcing, the provider has their own policy constraints, which are unlikely to map directly onto the processes defined in the OSCR framework.

  Response: the OSCR framework is intended to overcome existing security standards and frameworks weaknesses. In the event that the OSCR framework provides better security management, then the existing internal provider policies should not be a barrier to adopting

the OSCR framework. The change should be planned and implemented along the line of any other change (e.g. technology changes).

Action: No change to the OSCR framework.

- **Issue 2:** one of the key issues when outsourcing sensitive systems is where the data is kept and which legal jurisdiction applies to this data (some legal systems will override particular project agreements, which may undermine the OSCR framework).

  Response: where sensitive data are stored is outside the scope of the OSCR framework. Generally speaking, all project assets should be identified, including data. The security risks associated with the project assets should then be identified and assessed. Following that, security controls that mitigate the identified security risks should be put into practice. Contract conditions and other agreements (e.g. SLAs or NDAs) could enhance the security controls and reduce the potential security risks. If there are any exceptions, they should be managed through the Change Requests Unit.

  Action: No change to the OSCR framework.

- **Issue 3:** the one-size-fits-all approach is not practical given that the types and sizes of outsourced projects change over time.

  Response: the OSCR framework is not a one-size-fits-all approach. It is an asset-based approach, and was designed to be independent from different constraints such as the project type, cost or size. The rationale behind this is to provide a general methodology that can be tailored to fit any project based on the project assets rather than on project type or size. In this methodology, the need to develop different frameworks to fit different project types, sizes, costs, and missions is eliminated.

  Action: No change to the OSCR framework.

- **Issue 4:** the framework should clearly allow for new security risks to be added to the initial scope on an ongoing basis.

  Response: in spite of the fact that adding new security risks is managed through the Threat Classification Unit, its description did not

explain this clearly. The name of this unit also might confuse users of the OSCR framework.

Action: the description of the Threat Classification Unit was updated to explain how to add new security risks throughout project execution. Moreover, the Threat Classification Unit was renamed the Threat Identification Unit to provide a clearer meaning of this unit.

- **Issue 5:** mapping between the Plan-Do-Check-Act (PDCA) model and the project lifecycle is not clear.

  Response: in the PDCA model, the plan stage involves planning how to deliver the desired outputs of the project that meet the client's business needs. This stage reflects exactly what the planning phase does in the OSCR framework. The 'Do' stage is designed to allow the plans developed in the previous stage to be carried out. The execution phase in our framework represents this stage of the PDCA model. The 'Check' stage involves evaluating performance in the 'Do' stage. The 'Act' stage is used to propose new changes if the performance evaluation in the previous stage shows that the plans developed in the plan stage will not achieve the desired outputs. Those two stages are represented by the monitoring and controlling phase in the OSCR framework.

  Action: the description of the OSCR framework was updated to explain how the PCDA model is mapped to the OSCR framework phases (Appendix B).

3. *What improvements could be made to the* OSCR *framework in order to increase its ability to manage the security risks of outsourcing more effectively?*

   - **Recommendation 1**: a clear exceptions process is required where business drivers force deviation from security policies.

     Response: although exceptions that have not been analysed and assessed may threaten the entire organisation's security, there might be a need to allow exceptions to take place where they are required

(e.g. due to cost constraints). Nevertheless, they must be controlled and kept to the minimum.

Action: the objectives of the Change Requests Unit are updated to process exceptions in a controlled manner.

- **Recommendation 2**: It is advised that a third-party is assigned to the task of periodically auditing the compliance with the security requirements. Members of this audit team must be drawn from agencies not associated with the client in any way, to avoid conflict of interest or compromise of integrity.

  Response: the OSCR framework provides an approach for managing providers' compliance with the client security requirements. As the provider executes the project and the client audits the compliance through the project steering committee, there is no conflict of interest. However, external auditors could add a higher value of compliance if they are experienced and specialised in this domain.

  Action: No change to the OSCR framework.

- **Recommendation 3**: The implementation guidelines of the OSCR framework need to be improved. In an outsourcing environment, the time constraint needs to be considered. If the guidelines are not clear, this might affect the project master schedule as project team members may need more time to master the new processes of the OSCR framework.

  Response: during the introductory workshop, the OSCR framework was explained. The researcher was engaged with the participants during all implementation phases through different communication methods. Considering the absence of the researcher in the future use of the OSCR framework, there were some areas of the guidelines that need to be improved (e.g. Threat Identification Unit, Change Request Unit, and PDCA model).

  Action: the guidelines of how to implement the OSCR framework were updated to provide more information about how to apply the OSCR framework in the outsourcing context (Appendix B).

- **Recommendation 4:** roles and responsibilities in the OSCR framework should not allow name-based RACI (Responsible, Accountable, Consult, and Informed).

  Response: we utilised a role-based RACI method for assigning roles and responsibilities of project security activities in addition to the name-based RACI for use in some cases where project personnel are permanent (e.g. maintenance projects). For the purpose of outsourcing context, where personnel resources are not stable and might take part in the project activities in specific phases only (e.g. planning phase), it is true that the role-based RACI suits the context of outsourced projects more than name-based RACI. Even if the personnel are permanent, the role-based RACI will work fine.

  Action: the roles and responsibilities method used by the OSCR framework was updated to be only a role-based RACI method.

7.11 OSCR Framework Changes

In this section, we present all changes and improvements resulted from the all evaluation methods that we used to evaluate the OSCR framework (focus group, questionnaire, and case study). The final version of the OSCR framework is presented in Figure 7.1. The following summarises these changes and improvements:

7.11.1 Security Mitigations Unit (Initiating Phase)

The aim of this new unit is to propose and implement security controls that can be used to mitigate the potential security risks that might take place while executing the project. These potential security risks are identified by the client through the Potential Security Risks Unit.

7.11.2 Assets Unit (Planning Phase)

The project assets categories (Software, Hardware, Network, and Information) of the OSCR framework were updated to include human element.

Human is considered as a risk which should be identified and assessed along other assets risks.

7.11.3 Threat Identification Unit (Planning Phase)

The aim of this updated unit is to identify security threats using the outsourcing threat classification approach. The description of the Threat Classification Unit did not explain this clearly. The name of this unit also might confuse users of the OSCR framework. Therefore, the name was changed to Threat Identification Unit.

7.11.4 Compliance Requirements Unit (Planning Phase)

The aim of this new unit is to plan the requirements for compliance that will be audited during the monitoring and controlling phase by the project steering committee.

7.11.5 Roles and Responsibilities Unit (Planning Phase)

The role-based RACI method for assigning roles and responsibilities of project security activities will be the only method used by the OSCR framework. Name-based RACI will not be used as personnel resources of outsourced projects are usually not stable and might take part in the project activities in specific phases only (e.g. planning phase). The role-based RACI suits the context of outsourced projects more than name-based RACI. Even if the personnel are permanent, the role-based RACI will work fine.

7.11.6 Change Requests Unit (Executing Phase)

A new objective was added to this unit to process exceptions in a controlled manner as there might be a need to allow exceptions to take place where they are required. The original name and objectives for this unit are still the same without any change.

7.11.7 Compliance Auditing Unit (Monitoring & Controlling Phase)

The aim of this new unit is to audit compliance requirements planned in the Compliance Requirements Unit. This will increase the OSCR's ability to manage compliance more accurately, according to what has been planned, rather than depending on the auditors' effort, which might vary from one auditor to another.

7.11.8 Compliance Acceptance Unit (Closing Phase)

The aim of this updated unit is to accept or reject the provider's compliance with security requirements based on a project steering committee assessment resulting from the Compliance Auditing Unit.

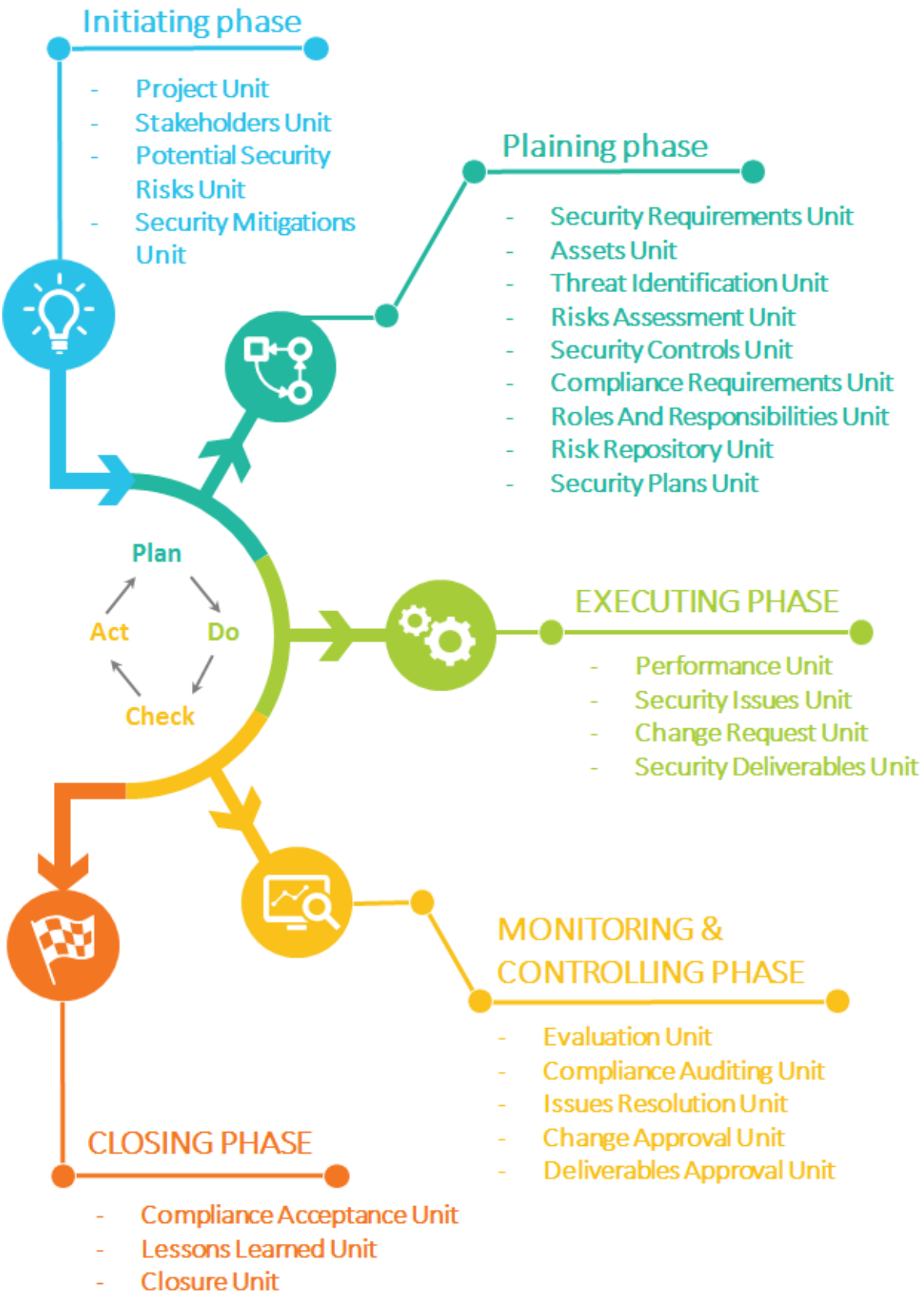

Figure 7.1: OSCR Framework-Final version

7.12 Discussion

In this section we will compare the OSCR framework with the existing ISMS standards and frameworks that we reviewed in Chapter 3. As can be seen in Table 7.5, we applied the same criteria (Sub-section 3.3.1) to the OSCR framework. The result shows that the OSCR framework provides better security and compliance risk management for the consideration of outsourced projects and usability criteria when compared with the information security management theme (e.g. ISO/IEC 2700x series, NIST SP 800 series, GMITS). For the IT governance and service management theme (e.g. COBIT, ITIL), the OSCR framework outperforms it in three criteria: risk management, consideration of outsourced projects and usability. The OSCR framework also provides better security and compliance risk management, when compared with the risk management theme (e.g. OCTAVE, CORAS, CRAMM), in all criteria except the usability criterion. For the security architecture and engineering theme (e.g. SABSA, SSE-CMM), the OSCR framework achieves better security and compliance risk management in two criteria: consideration of outsourced projects and usability.

Table 7.5: OSCR Framework Comparison with ISMSs

Criteria	***ISO/IEC 2700x series***	***NIST SP 800 - series***	***GMITS***	***COBIT***	***ITIL***	***OCTAVE***	***CORAS***	***CRAMM***	***SABSA***	***SSE-CMM***	***OSCR Framework***
1-Security Requirements Management:											
Information Security Policy	√	√	√	√	√	×	×	×	√	√	√
Communications and Operations Management	√	√	√	√	×	≈	×	×	√	√	√
Access Control	√	√	≈	√	√	×	×	×	√	√	√
Information Systems Acquisition, Development, and Maintenance	√	√	√	√	×	×	×	×	√	√	√

Criteria	***ISO/IEC 2700x series***	***NIST SP 800 - series***	***GMITS***	***COBIT***	***ITIL***	***OCTAVE***	***CORAS***	***CRAMM***	***SABSA***	***SSE-CMM***	***OSCR Framework***
Asset Management	√	√	≈	√	√	√	√	√	√	√	√
Incident Management	√	√	√	√	√	×	×	×	≈	≈	√
Business Continuity Management	√	√	√	√	√	×	×	×	√	≈	√
2- Risks Management:											
Physical and Environmental Risks	√	√	√	≈	×	≈	≈	≈	√	√	√
Human Resources Risks	√	√	√	≈	×	≈	≈	≈	√	√	√
Technical Risks	√	√	√	≈	≈	√	√	√	√	√	√
3- Consideration of outsourced projects:	≈	≈	≈	×	×	×	×	×	≈	×	√
4- Compliance	√	√	√	√	√	×	×	×	√	√	√
5- Usability:											
Cost effectiveness	×	×	×	×	×	√	√	√	×	×	√
Time efficiency	×	×	×	×	×	√	≈	√	×	×	√
Simplicity and easiness	×	×	×	×	×	√	√	√	×	×	√

Table 7.6: OSCR Framework Comparison with ISMSs - Summary

	ISO/IEC 2700x series	***NIST SP 800 - series***	***GMITS***	***COBIT***	***ITIL***	***OCTAVE***	***CORAS***	***CRAMM***	***SABSA***	***SSE-CMM***	***OSCR Framework***
Count											
√	*11*	*11*	*9*	*8*	*6*	*5*	*4*	*5*	*10*	*9*	*15*
≈	*1*	*1*	*3*	*3*	*1*	*3*	*3*	*2*	*2*	*2*	*0*
×	*3*	*3*	*3*	*4*	*8*	*7*	*8*	*8*	*3*	*4*	*0*
Percentage											
√	73%	73%	60%	53%	40%	33%	27%	33%	67%	60%	100%
≈	7%	7%	20%	20%	7%	20%	20%	13%	13%	13%	0%
×	20%	20%	20%	27%	53%	47%	53%	53%	20%	27%	0%

7.13 Summary

In this chapter, we have presented the empirical evaluation method that we used to evaluate the novelty of the OSCR framework in managing the security and compliance risks of outsourced IT projects. It was decided to use a case study in evaluating the OSCR framework due to the several benefits of using the case study such as the rich and in-depth data that can be obtained and the practical knowledge and experience of the participants who took part in this evaluation.

As a case study, we have used two outsourced IT projects. The aim of this case study was to assess the ability of the OSCR framework to manage the security and compliance risks of IT projects in outsourcing context effectively. It was also aimed to discover potential changes and improvements that could enhance the OSCR framework performance when outsourcing IT projects.

According to the case study results, the participants acknowledged that the OSCR framework provided them with an effective approach for managing security and compliance risks in the outsourcing context. In comparison with what they use currently (e.g. ISO2700x, COBIT5, etc.), the OSCR framework was better and covered all required security aspects that need to be considered when outsourcing. It was understandable, simple and easy to use and independent from different constraints such project size, cost, or execution time.

Based on the evaluation results, the OSCR framework was updated to accommodate the case study observations and the participants' suggestions and improvements that are believed to improve the ability of the OSCR framework to effectively manage the security and compliance risks of outsourced IT projects.

Finally, we revisited the evaluation criteria that we used in Chapter 3 to evaluate the existing ISMS standards and frameworks. The OSCR met all the criteria and achieved better management of the security and compliance risks of outsourced IT projects in comparison with these ISMS standards and frameworks.

In the following chapter, a summary of this thesis, research contributions, limitations, and future work will be provided.

Chapter 8 Conclusion and Future Work

8.1 Introduction

In the previous chapter, the OSCR framework was evaluated using a case study. In this chapter a summary of this thesis, research contributions, limitations and future work will be presented. The research findings are provided and linked to the research questions to show how each research question has been answered.

8.2 Research Summary

Outsourcing has been adopted by many organisations as the principal means of delivering critical IT services for themselves and their clients. On the one hand, outsourcing offers organisations a great deal of benefits such as cost reductions, quality improvements and access to the latest technology. On the other hand, it brings them different security risks such as confidentiality, integrity, and availability risks.

The lack of a comprehensive methodology that is capable of effectively managing the security and compliance risks of outsourced IT projects was one of the motivations for this research. The main objective of this research was to develop a framework for managing the security and compliance risks of outsourced IT projects. The main question and two sub-questions asked in this research are:

1- *How can we manage the security and compliance risks of outsourced IT projects effectively?*

- ***a.*** *What are strengths and weaknesses of the existing security standards and frameworks for managing the security and compliance risks of outsourced IT projects?*
- ***b.*** *What are the requirements for managing the security and compliance risks of outsourced IT projects?*

In order to answer the research questions and achieve the research objectives, a research methodology was developed and put into practice. According to the research methodology, the work started by reviewing the literature related to outsourcing (presented in Chapter 2). The aim was to provide background information related to outsourcing business practice. Different benefits can be offered by outsourcing. Cost reductions, concentration on core business activities, flexibility and quality improvement, and minimising routine tasks and obsolescence risk, are examples of such benefits. Despite the enormous benefits that outsourcing can offer organisations, it might expose organisations to different risks such as security risks and contract violations.

Security risks associated with outsourcing led to the need to review existing ISMS standards and frameworks to assess their ability to manage these risks. This review represents the second step in the research methodology. For this purpose, specific criteria were identified and followed. We proposed five specific criteria for this review: security requirements management, risks management, consideration of outsourced projects, compliance management, and usability. To provide a more precise coverage of the review, each criterion is further decomposed into elements.

As presented in Chapter 3, existing ISMSs standards and frameworks are categorised into four themes: information security management, IT governance and service management, risk management, and security architecture and engineering. Representative examples of ISMSs standards and frameworks were provided and reviewed based on the proposed criteria. The review results show that existing ISMSs have some limitations with regard to managing security risks in the outsourcing context. The lack of comprehensive methodology, low usability, generality, and the lack of adequate consideration of outsourced projects are examples of these limitations.

To manage the security and compliance risks of outsourced IT projects effectively, specific requirements and needs were identified as a result of the literature and the ISMSs reviews. The requirements and needs identification

represents the third step in the research methodology. As presented in Chapter 4, the requirements were aligning security management with project management, establishing a comprehensive methodology for managing security requirements, managing security risks from different perspectives, managing compliance, improving flexibility and usability and enhancing reusability.

In response to these requirements and needs, we proposed a framework called the OSCR framework (Outsourcing Security and Compliance Risks framework) for managing the security and compliance risks of outsourced IT projects, which represents the fourth step in the research methodology. As presented in Chapter 5, the framework utilises project phases (initiating, planning, execution, monitoring and controlling, and closing) and the PDCA model. Each project phase has its own security processes. During the planning, execution, and monitoring and controlling phases, the PDCA model is applied.

The framework uses a hybrid threat classification approach that is designed for the outsourcing context, in which environments are less stable and more systems are integrated. It combines different threat classification criteria and considers threats from different perspectives such as external threats, provider threats, client threats, and physical and environmental threats.

Evaluating the OSCR framework was the last step of the research methodology. The OSCR framework was evaluated using two empirical methods. The first method, as presented in Chapter 6, was a focus group and a questionnaire. The aim of this evaluation was to identify any potential weaknesses that the OSCR framework might have, as well as drawing out ideas and recommendations from the relevant people involved in outsourcing who could contribute to improving the OSCR framework. Valuables ideas and recommendations were received from the participants and considered before conducting the case study.

Having considered the ideas and recommendations from the first evaluation method and carrying out the required updates, the OSCR framework has been

applied to real outsourced IT projects as presented in Chapter 7. It was decided to use a case study in order to evaluate the OSCR framework as this had several benefits, such as the rich and in-depth data that can be obtained and the practical knowledge and experience of the participants who took part in this evaluation. The case study allowed us to investigate the ability of the OSCR framework to manage the security and compliance risks of outsourced IT projects effectively in their "real-life" context.

8.3 Answers to the Research Questions

In this section, we will discuss the research questions and explain how they were answered in this research. Each question will be stated and followed by the required explanation.

1. *How can we manage the security and compliance risks of outsourced IT projects effectively?*

This question represents the main question of this research. Two sub-questions were prepared and asked in order to answer the main research question as follows.

a) *What are strengths and weaknesses of the existing security standards and frameworks for managing the security and compliance risks of outsourced IT projects?*

To answer this question, and based on the aim of this research and the outcome of the literature review, we proposed five specific criteria for reviewing the existing ISMS standards and frameworks as presented in Chapter 3.

The main weaknesses resulting from the review are summarised as follows:

- Lack of or weak comprehensive security methodology: this was a limitation of the majority of the ISMSs reviewed. They tended to provide only general recommendations and gave no detailed instructions for their application.

- Lack of or weak consideration of compliance management: the majority of the ISMSs reviewed failed to supply guidance on how organisations could enforce compliance with security requirements.

- Usability: the usability issue with a large part of the reviewed ISMSs was that in order to implement them effectively, the organisation would need access to a large bank of resources. When outsourcing, budget constraints and adhering to the project schedule are important, therefore ease of use, cost effectiveness, simplicity and time efficiency are paramount.

- Generality: The suggestions provided by existing ISMSs are general and they do not take into account the variety of security requirements that exists in different organisations. They lack explanations of how to apply the suggestions given, and in which situations they apply.

- Lack of adequate consideration of outsourced projects: On the whole, ISMSs are designed with organisations' internal processes in mind, not the challenges and risks associated with outsourced IT projects. These risks are rarely mentioned, and if they are, they are only addressed very generally and there are no detailed guidelines on how to deal with them.

Following the review, the following conclusions were drawn:

- No one standard or framework is able to satisfy all the required criteria.

- The ISMSs reviewed in this research were clearly not designed specifically for the management of the security and compliance risks of outsourced IT projects. Attempting to update them so that they could be applied to this type of project would increase their complexity, and consume valuable time and resources.

- The strengths and weaknesses of the different standards and frameworks reviewed here differ considerably. For example, OCTAVE is characterised by high usability but low security requirements management, and ISO/IEC 2700x is the opposite, with high security requirements management but

low usability. A new proposed framework should build on these strengths while aiming to reduce the weaknesses.

- All of the frameworks and standards reviewed suffered from poor usability.

b) *What are the requirements for managing the security and compliance risks of outsourced IT projects?*

As presented in Chapter 4, the following requirements need to be taken into consideration when outsourcing in order to manage the security risks of outsourcing more effectively:

- Aligning Security Management with Project Management: this may enable separate security risk management, which in turn could facilitate greater understanding of security requirements. Resources may then be freed for use on other project activities.
- Managing Security Requirements: the security programme or framework employed by an organisation to assess the risks of outsourcing projects should comprise a complete and clear methodology. Organisations can then confidently identify their security requirements, the first step towards managing them. All of the factors (e.g. security policy, access list…etc.) that are part of a comprehensive security programme or framework should be considered.
- Managing Security Risks: the security programme or framework should identify and manage the risks that arise from different perspectives (e.g. technical, human…etc.).
- Managing Compliance: the security programme or framework should provide guidelines on effectively enforcing compliance.
- Improving Usability: the security programme or framework should provide high usability from different perspectives (e.g. cost effectiveness, time efficiency….etc.).

- Supporting Flexibility: The security programme or framework should incorporate a degree of flexibility so that any changes that occur can be accommodated.
- Enhancing reusability: Within the same organisation, outsourced IT projects may share several common elements, such as environments, assets, etc. It is clearly a waste of resources to spend time repeating tasks that do not need to be repeated, therefore being able to reuse previous threat identification and risk assessment results is a great benefit, as it frees up resources for other parts of the project and speeds up the process.

Based on the outcomes of answering the two sub-questions, we have developed the OSCR framework for managing the security and compliance risks of outsourced IT projects as a response for the main question of the research. As presented in Chapter 5, the OSCR framework meets all the requirements that have been identified for managing the security and compliance risks of outsourced IT projects.

In comparison with existing ISMS standards and frameworks, the OSCR framework has met all the five criteria that were used to evaluate the ISMSs in Chapter 3. When considering the first criterion (security requirements management), the OSCR framework outperformed the risk management theme approaches (e.g. OCTAVE), but did not provide a big improvement compared to the other three themes: information security management (e.g. ISO/IEC 2700x series), IT governance and service management (e.g. ITIL) and security architecture and engineering (e.g. SABSA). Focusing on the second criterion (risk management), the OSCR framework is as good as the approaches of the information security management, security architecture and engineering themes, but provides better performance than the approaches of the IT governance and service management, and risk management themes. When looking at the third criterion (consideration of outsourced project), the OSCR framework provides better performance than the approaches of all the themes. In the fourth criterion

(compliance), the OSCR outperforms the approaches of the risk management theme. But it performs better than all the approaches of all the themes when focusing on the last criterion (usability), except the approaches of the risk management theme.

The research main question (how can we manage the security and compliance risks of outsourced IT projects?) is answered by the development of the OSCR framework. The evaluation of the OSCR framework assessed the effectiveness of the solution (the framework) with regard to its ability to manage the security and compliance risks of outsourced IT projects.

8.4 OSCR Framework Evaluation

The main evaluation methods that we used to evaluate the novelty and the ability of the OSCR framework to manage security and compliance risks effectively were a focus group, a questionnaire, and a case study.

The evaluation methods were planned in such a way that they covered different aspects of the OSCR framework. The following highlight the aspects that were targeted during the evaluation:

- Evaluating the general architecture of the OSCR framework, including the outsourcing threat classification approach, which was designed for the outsourcing context.
- Assessing the ability of the OSCR framework to effectively manage the security and compliance risks of outsourced IT projects.
- Evaluating the OSCR framework's coverage of security aspects that need to be taking into consideration in the outsourcing context.
- Comparing the OSCR framework with related ISMS standards and frameworks.
- Gathering recommendations from expert people in outsourcing that could be used to improve the OSCR framework.
- Evaluating the achievement of the promising features of the OSCR framework (e.g. simplicity, undependability, flexibility).

1- Focus Group and Questionnaire

Six focus group workshops were conducted and complemented with an online questionnaire. The participants (programme manager, project manager, project team member, PMO officer, security specialist, IT architect, or applications developer) have relevant experience in outsourced IT projects and related areas such as security and applications development.

As presented in Chapter 6, the evaluation results show that the OSCR framework has achieved a high acceptance in the outsourcing context. Several features such as flexibility, simplicity and ease of use have been confirmed by the participants. It was agreed by the participants that the framework provides a comprehensive methodology that is capable of providing organisations with the ability to minimise or mitigate security risks in the early stages of project execution. It is also acknowledged by the participants that the OSCR framework is strengthened by a robust threat classification approach that improves threat identification in the outsourcing context. The PDCA model provides a continuous improvement process to accommodate the changes and improvements required while executing the project.

The results of this evaluation were used to update the OSCR framework to reflect some valuable recommendations from the participants (e.g. compliance management, potential security risk mitigations). They were suggested to improve the OSCR framework's ability to manage security and compliance risks in a more effective way in the outsourcing context.

2- Case Study

As the OSCR framework had been revised and improved based on the outcome from the focus group and the questionnaire, as well as publication feedback, the framework was put into practice. As a case study, we used two outsourced IT projects. The OSCR framework was applied to the two outsourced IT projects from the beginning of the projects' execution until their end.

As presented in Chapter 7, the case study results confirmed that the OSCR framework provided the participants with an effective approach for managing security and compliance risks in the outsourcing context. In comparison with what they use currently (e.g. ISO2700x, COBIT5, etc.), the OSCR framework was better and covered all the required security aspects that needed to be considered when outsourcing. It was understandable, simple and easy to use and independent from different constraints such project size, cost, or execution time. Finally, the OSCR framework was updated to accommodate the case study observations and the participants' suggestions and improvements.

8.5 Research Contributions

The OSCR framework that is to be used for managing the security and compliance risks of outsourced IT projects represents the major contribution of this research. Also, the review of existing ISMS standards and frameworks provides an assessment of these ISMSs in the outsourcing context and identifies their strengths and weaknesses. Other contributions include the analysis of outsourcing business practice, the threat classification approach, and the research publications. The following provides more details about these contributions.

1- The OSCR Framework

The OSCR framework contributes to the knowledge body as follows:

- Developing a comprehensive methodology for security and compliance risks management in the outsourcing context.
- Introducing the concept of aligning security management with project management.
- Identifying security processes that need to be used when outsourcing. Each phase of the OSCR framework consists of specific processes that add value for security and compliance risk management.

- Designing an outsourcing threat classification approach that suits the outsourcing context, where different parties are involved in the project execution.
- Considering flexibility and continuous improvements by utilising the PDCA model.
- Improving adherence to security requirements. This is essential as without it, there is a danger that the security requirements will not be fulfilled.
- Achieving promising features. The evaluators acknowledged several useful features of the OSCR framework, for example it was simple and easy to use, and they valued its flexibility and reusability.

2- ISMSs Review

Existing ISMSs have been reviewed and analysed in this research. The review classified existing ISMSs into four themes and identified their weaknesses, strengths and main focus. Based on the review outcome, the existing ISMSs still have weaknesses that affect their ability to manage the security and compliance risks of outsourced IT projects effectively.

3- Outsourcing Analysis

Outsourcing business practice has been analysed as it was important to understand this business practice, its benefits, risks, and so on. This allowed us to identify challenges and needs for managing the security and compliance risks of outsourced IT projects effectively. The analysis showed that despite the enormous benefits that outsourcing could offer organisations; it might expose organisations to different security risks such as confidentiality, integrity, and availability risks.

4- Research Publications

Our aim was to publish the findings from this research at a number of relevant conferences. We successfully published six publications on various

aspects of the research, including the OSCR framework, the review of ISMSs and the outsourcing threat classification approach.

8.6 Research Limitations

In spite of the fact that the OSCR framework contributes significantly to providing a comprehensive and effective methodology for managing the security and compliance risks of outsourced IT projects, there are still some limitations. The following highlights them briefly:

- The case study was limited in terms of the number and type of projects due to several constraints (e.g. research time, cost…etc.).
- The case study (the two projects) was conducted in a single client environment. It would have been better to conduct it at different clients in order to assess the OSCR framework in different environments and with different security practices. This limitation was due to several constraints (e.g. client willingness, privacy issues, execution time…etc.).
- The questionnaire was limited in terms of the participants' numbers. This was due to the difficulty of finding experienced candidates in security management for outsourced IT projects within the research time frame.
- The OSCR framework does not come with a software tool for automating paperwork. Having such a tool would speed up the process and allow projects teams to access project data in a more convenient way.
- There were no major security incidents during the case study implementation. Although it was not practical to create one, it would have been better if we had experienced at least one and been able to present the OSCR framework's ability to handle the security changes in response to the security incident using the PDCA model.

8.7 Future Work

Despite the research limitations presented in the previous section, we assert that this research has largely achieved its objectives. A comprehensive approach (the OSCR framework) was developed for managing security and compliance risks in outsourcing. Based on the evaluation results, the OSCR framework provides a powerful approach capable of managing the security and compliance risks in the outsourcing context. We think that there are still some opportunities to improve this work. The following give some directions for these opportunities:

- The OSCR framework could be initiated with a list of potential security and compliance risks that might take place when outsourcing. The outsourcing threat classification approach that we developed in this research could be used for this purpose. Many security risks are common (e.g. DoS) and can take place in different environments. This list could reduce the amount of work required for the risk identification process.
- The OSCR framework could be enhanced by a software tool to automate the framework processes. This will reduce the paperwork time and provide a wider ability to access the project data.
- The OSCR framework could be evaluated in different environments with different clients. More projects that differ in their size, type or mission might be used. This will provide more comments and recommendations to improve the OSCR framework.
- The OSCR framework could be evaluated using a simulation of major security incidents if a real one is not experienced.
- The OSCR framework was designed for conventional outsourcing contexts. However, we suggest that it could be generalised to other outsourcing contexts such as cloud computing and offshoring. More study and evaluation need to be conducted to determine the needs and challenges for these contexts.

References

[1] H. Min, S.-J. Joo, and T. S. Nicolas-Rocca, "Information system outsourcing and its impact on supply chain performances," *International Journal of Logistics Systems and Management,* vol. 24, no. 4, pp. 409-425, 2016.

[2] D. Bachlechner, S. Thalmann, and R. Maier, "Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective," *Computers & Security,* vol. 40, pp. 38-59, 2014.

[3] M. J. Creon, V. Grover, and J. T. Teng, "Theoretical Perspectives on the Outsourcing of Information Systems," in *Outsourcing and Offshoring Business Services*: Springer, pp. 25-52, 2017.

[4] J. Dibbern, T. Goles, R. Hirschheim, and B. Jayatilaka, "Information systems outsourcing: a survey and analysis of the literature," *ACM Sigmis Database,* vol. 35, no. 4, pp. 6-102, 2004.

[5] C. Brandas, "Risks and audit objectives for IT outsourcing," *Informatica Economica Journal,* vol. 14, no. 1, pp. 113-118, 2010.

[6] K. Han and S. Mithas, "Information Technology Outsourcing and Non-IT Operating Costs: An Empirical Investigation," *MIS Quarterly,* vol. 37, no. 1, pp. 315-331, 2013.

[7] R. Gonzalez, J. Gasco, and J. Llopis, "Information systems outsourcing reasons and risks: an empirical study," *International Journal of Human and Social Sciences,* vol. 4, no. 3, pp. 181-192, 2009.

[8] C. Schwarz, "Toward an understanding of the nature and conceptualization of outsourcing success," *Information & Management,* vol. 51, no. 1, pp. 152-164, 2014.

[9] R. Gonzalez, J. Gasco, and J. Llopis, "Information systems outsourcing risks: a study of large firms," *Industrial management & Data systems,* vol. 105, no. 1, pp. 45-62, 2005.

[10] R. Gonzalez, J. Gasco, and J. Llopis, "Information systems outsourcing reasons and risks: a new assessment," *Industrial Management & Data Systems,* vol. 110, no. 2, pp. 284-303, 2010.

[11] J. Iqbal, R. Binti Ahmad, and M. A. Noor, "Frequently occurring risks for IT outsourcing projects," in *International Conference on Computer and Communication Engineering (ICCCE)*, pp. 957-960, 2012.

[12] B. M. Bhatti, S. Mubarak, and S. Nagalingam, "A framework for information security risk management in IT outsourcing," 2017.

[13] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & Management,* vol. 46, no. 5, pp. 267-270, 2009.

[14] T. Wiander, "Positive and negative findings of the ISO/IEC 17799 framework," *ACIS 2007 Proceedings,* p. 75, 2007.

[15] X. Xi, Y. Xu, and H. Todo, "The Present Situation of IT Outsourcing and Countermeasure," *Journal of Software Engineering and Applications,* vol. 6, no. 8, pp. 426-430, 2013.

[16] R. Ross, P. Viscuso, G. Guissanie, K. DEMPSEY, and M. Riddle, "Protecting controlled unclassified information in nonfederal information systems and organizations," *NIST Special Publication,* vol. 800, p. 171, 2015.

[17] C. LOGICAL, "Information technology–Security techniques–Information security management systems–Requirements," 2005.

[18] Ü. Tatar and B. Karabacak, "An hierarchical asset valuation method for information security risk analysis," in *International Conference on Information Society (i-Society)*, pp. 286-291, 2012.

[19] E. Aroms, "NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems," 2012.

[20] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *eighth international conference on Availability, reliability and security (ares)*, pp. 546-555, 2013.

[21] J. Granneman, "IT security frameworks and standards: Choosing the right one," *TechTarget,* 2013.

[22] M. M. Eloff and S. H. von Solms, "Information security management: a hierarchical framework for various approaches," *Computers & Security,* vol. 19, no. 3, pp. 243-256, 2000.

[23] I. Oshri, J. Kotlarsky, and L. P. Willcocks, *The Handbook of Global Outsourcing and Offshoring 3rd Edition*. Palgrave Macmillan, 2015.

[24] J. W. Ross and G. Westerman, "Preparing for utility computing: The role of IT architecture and relationship management," *IBM systems journal,* vol. 43, no. 1, pp. 5-19, 2004.

[25] A.-M. Majanoja, L. Linko, and V. Leppänen, "Developing offshore outsourcing practices in a global selective outsourcing environment–the IT supplier's viewpoint," 2017.

[26] N. Gorla and T. M. Somers, "The impact of IT outsourcing on information systems success," *Information & Management,* vol. 51, no. 3, pp. 320-335, 2014.

[27] R. Morgan and D. Doran, "The evolving dynamics of outsourcing: control and conflict a vendors perspective," in *21st EurOMA Conference: Conference Book Programme and Abstracts*, 2014.

[28] M. Akbari, S. Clarke, and S. M. Far, "Outsourcing best practice-the case of large construction firms in Iran," in *SITE 2017*: Informing Science Institute, pp. 39-50, *2017*.

[29] M. Rekik, K. Boukadi, and H. Ben-Abdallah, "A decision-making method for business process outsourcing to the cloud based on business motivation model and AHP," *International Journal of Cloud Computing 2,* vol. 4, no. 1, pp. 47-62, 2015.

[30] L. van Scheers, "Managing The Risk Of Outsourcing The IT Functions At Companies," *RISK GOVERNANCE & CONTROL: Financial markets and institutions,* pp. 69-74, 2016.

[31] M. Pellicelli, "From Outsourcing and Offshoring Strategies to Extreme Outsourcing," *Economia Aziendale Online,* vol. 8, no. 1, pp. 33-44, 2017.

[32] H. Smuts, P. Kotzé, A. van der Merwe, and M. Loock, "Threats and opportunities for information systems outsourcing," in *2015 International Conference on Enterprise Systems (ES)*, pp. 110-120, 2015.

[33] A. Vaxevanou and N. Konstantopoulos, "Basic Principles the Philosophy of Outsourcing," *Procedia-Social and Behavioral Sciences,* vol. 175, pp. 567-571, 2015.

[34] G. Tayauova, "Advantages and disadvantages of outsourcing: analysis of outsourcing practices of Kazakhstan banks," *Procedia-Social and Behavioral Sciences,* vol. 41, pp. 188-195, 2012.

[35] T. Ackermann, A. Miede, P. Buxmann, and R. Steinmetz, "Taxonomy of technological IT outsourcing risks: support for risk identification and quantification," in *ECIS*, 2011.

[36] X. Zhu, "Management the risks of outsourcing: Time, quality and correlated costs," *Transportation Research Part E: Logistics and Transportation Review,* pp. 121-133, 2016.

[37] R. McIvor, "What do we know about services outsourcing," *Institute of Chartered Accountants of Scotland, Edinburgh,* 2013.

[38] R. González, J. Gascó, and J. Llopis, "Information Systems Outsourcing Reasons and Risks: Review and Evolution," *Journal of Global Information Technology Management,* vol. 19, no. 4, pp. 223-249, 2016.

[39] J. Rhodes, P. Lok, W. Loh, and V. Cheng, "Critical success factors in relationship management for services outsourcing," *Service Business,* vol. 10, no. 1, pp. 59-86, 2016.

[40] A. Zimmermann and M. Ravishankar, "A systems perspective on offshoring strategy and motivational drivers amongst onshore and offshore employees," *Journal of World Business,* vol. 51, no. 4, pp. 548-567, 2016.

[41] B. Dorsemaine, J.-P. Gaulier, J.-P. Wary, N. Kheir, and P. Urien, "A new threat assessment method for integrating an IoT infrastructure in an information system," in *37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 105-112, 2017

[42] A.-M. Dinu, "The Risks and Benefits of Outsourcing," *Knowledge Horizons. Economics,* vol. 7, no. 2, pp. 103-104, 2015.

[43] G. Nassimbeni, M. Sartor, and D. Dus, "Security risks in service offshoring and outsourcing," *Industrial Management & Data Systems,* vol. 112, no. 3, pp. 405-440, 2012.

[44] R. Elitzur, A. Gavious, and A. K. Wensley, "Information systems outsourcing projects as a double moral hazard problem," *Omega,* vol. 40, no. 3, pp. 379-389, 2012.

[45] F. Ahmed, L. F. Capretz, M. A. Sandhu, and A. Raza, "Analysis of risks faced by information technology offshore outsourcing service providers," *IET Software,* vol. 8, no. 6, pp. 279-284, 2014.

[46] J. Słoniec, A. Kaczorowska, and S. Motyka, "Risk assessment of IT outsourcing in enterprises depending on their branch," *technology,* vol. 11, pp. 473-486, 2016.

[47] A. Gunasekaran, Z. Irani, K.-L. Choy, L. Filippi, and T. Papadopoulos, "Performance measures and metrics in outsourcing decisions: A review for research and applications," *International Journal of Production Economics,* vol. 161, pp. 153-166, 2015.

[48] G. Dhillon, R. Syed, and F. de Sá-Soares, "Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors," *Information & Management,* vol. 54, no. 4, pp. 452-464, 2017.

[49] J. Moon, C. Lee, S. Park, Y. Kim, and H. Chang, "Mathematical model-based security management framework for future ICT outsourcing project," *Discrete Applied Mathematics,* vol. 241, pp. 67-77, 2016.

[50] K. W. Hamlen and B. Thuraisingham, "Data security services, solutions and standards for outsourcing," *Computer Standards & Interfaces,* vol. 35, no. 1, pp. 1-5, 2013.

[51] T. Bandyopadhyay, D. Beyene, and S. Negash, "IT outsourcing risk management practices in higher educational institutes in Ethiopia–A qualitative study," *in Twenty-first Americas conference on information systems,* 2015.

[52] A. Alfantookh, "An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls," *Computer Sciences, King Saud University,* 2009.

[53] H. Susanto and F. bin Muhaya, "Multimedia information security architecture framework," in *5th International Conference on Future Information Technology (FutureTech)*, pp. 1-6, 2010.

[54] W. Ismail, N. H. M. Alwi, R. Ismail, M. Bahari, and O. Zakaria, "Readiness of Information Security Management Systems (ISMS) Policy on Hospital

Staff Using e-Patuh System," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* vol. 10, no. 1-11, pp. 47-52, 2018.

[55] S. M. Ali, "Integration of information security essential controls into information technology infrastructure library-A proposed framework," *International Journal of Applied Science and Technology,* vol. 4, no. 1, pp. 95-100, 2014.

[56] Y. Benslimane, Z. Yang, and B. Bahli, "Information Security between Standards, Certifications and Technologies: An Empirical Study," in *International Conference on Information Science and Security (ICISS)*, pp. 1-5, 2016.

[57] K. Haufe, R. Colomo-Palacios, S. Dzombeta, K. Brandis, and V. Stantchev, "A process framework for information security management," *International Journal of Information Systems and Project Management,* vol. 4, no. 4, pp. 27-47, 2016.

[58] L. Almeida and A. Respício, "Decision support for selecting information security controls," *Journal of Decision Systems,* vol. 27, no. sup1, pp. 173-180, 2018.

[59] S. B. von Solms, "Information Security Governance–compliance management vs operational management," *Computers & Security,* vol. 24, no. 6, pp. 443-447, 2005.

[60] H. Susanto and M. N. Almunawar, "Managing Compliance with an Information Security Management Standard," in *Encyclopedia of Information Science and Technology, Third Edition*: IGI Global, pp. 1452-1463, 2015.

[61] A. AlKalbani, H. Deng, B. Kam, and X. Zhang, "Investigating the impact of institutional pressures on information security compliance in organizations," *Australasian Conference on Information Systems,* 2016.

[62] A. Narain Singh, M. Gupta, and A. Ojha, "Identifying factors of "organizational information security management"," *Journal of Enterprise Information Management,* vol. 27, no. 5, pp. 644-667, 2014.

[63] H. Susanto12, M. N. Almunawar, and Y. C. Tuan, "Information security management system standards: A comparative study of the big five,"

International Journal of Electrical Computer Sciences IJECSIJENS, vol. 11, no. 5, pp. 23-29, 2011.

[64] T. Elliman, "Generating citizen trust in e-government using a trust verification agent: a research note," in *the European and Mediterranean Conference on Information Systems (EMCIS)*, 2006.

[65] T. Chmielecki *et al.*, "Enterprise-oriented cybersecurity management," in *Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 863-870, 2014.

[66] M. Nicho and S. Khan, "IT governance measurement tools and its application in IT-business alignment," *Journal of International Technology and Information Management,* vol. 26, no. 1, pp. 81-111, 2017.

[67] W. Al-Ahmad and B. Mohammad, "Addressing information security risks by adopting standards," *International Journal of Information Security Science,* vol. 2, no. 2, pp. 28-43, 2013.

[68] M. Tajammul and R. Parveen, "Comparative analysis of big ten ISMS standards and their effect on cloud computing," in *International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, pp. 362-367, 2017.

[69] A. Talea, K. El Guemmat, M. Talea, and A. Tragha, "Towards A New System of Selecting Information Systems Frameworks," *International Journal,* vol. 5, no. 12, 2015.

[70] E. Humphreys, "Information security management system standards," *Datenschutz und Datensicherheit-DuD,* vol. 35, no. 1, pp. 7-11, 2011.

[71] H. Susanto, M. N. Almunawar, and Y. C. Tuan, "Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level," *International Journal of Engineering and Technology. IJET Publications UK,* vol. 2, no. 1, 2012.

[72] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for information security management," *Journal of Information Security,* vol. 4, no. 2, pp. 92-100, 2013.

[73] J. G. Nowak, "Information Security Management with accordance to ISO27000 Standards: Characteristics, implementations, benefits in global Supply Chains," *Logistyka,* pp. 639-654, 2015.

[74] R. Sheikhpour and N. Modiri, "A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management," *Indian Journal of Science and Technology,* vol. 5, no. 2, pp. 2170-2176, 2012.

[75] S. Ristov, M. Gusev, and M. Kostoska, "A new methodology for security evaluation in cloud computing," in *MIPRO, Proceedings of the 35th International Convention*, pp. 1484-1489, 2012.

[76] A. MP Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "Technical security metrics model in compliance with ISO/IEC 27001 standard," *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 1, no. 4, pp. 280-288, 2012.

[77] A. L. Mesquida and A. Mas, "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension," *Computers & Security,* vol. 48, pp. 19-34, 2015.

[78] D. C. Tofan, "Information Security Standards," *Journal of Mobile, Embedded and Distributed Systems,* vol. 3, no. 3, pp. 128-135, 2011.

[79] M. Ndungu and S. Kandel, "Information Security Management In Organizations " 2015.

[80] J. Hallberg *et al.*, "Controlled Information Security," *FOI, Swedish Defence Research Agency,* pp. 1-42, 2011.

[81] V. Lalanne, M. Munier, and A. Gabillon, "Information security risk management in a world of services," in *International Conference on Social Computing (SocialCom)*, pp. 586-593, 2013.

[82] L. Rajbhandari, "Consideration of Opportunity and Human Factor: Required Paradigm Shift for Information Security Risk Management," in *European Intelligence and Security Informatics Conference (EISIC)*, pp. 147-150, 2013.

[83] M. Swanson, J. Hash, and P. Bowen, "NIST Special Publication 800-18 Revision 1," *Guide for Developing Security Plans for Federal Information Systems,* 2006.

[84] E. Aroms, "NIST Special Publication 800-18 Revision 1 Guide for Developing Security Plans for Federal Information Systems," 2012.

[85] E. A. Nist, "NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems," *CreateSpace, Paramount, CA,* 2012.

[86] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," *Information Management & Computer Security,* vol. 22, no. 5, pp. 410-430, 2014.

[87] M. Swanson, P. Bowen, W. Amy, D. Gallup, and D. Lynes, "NIST Special Publication 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems," *Swanson, P. Bowen, AW Phillips, D. Gallup, D. Lynes.–2010.–149 p,* 2010.

[88] R. Gandhi, K. Crosby, T.-G. R. Solutions, L. H. Siy, and S. Mandal, "Driving Secure Software Initiatives Using FISMA: Issues and Opportunities," in *CrossTalk*: US Department of Defense, p. 37, 2016.

[89] S. Park and K. Lee, "Advanced approach to information security management system model for industrial control system," *The Scientific World Journal,* 2014.

[90] P. H. Meland, I. A. Tondel, and B. Solhaug, "Mitigating risk with cyberinsurance," *IEEE Security & Privacy,* vol. 13, no. 6, pp. 38-43, 2015.

[91] P. J. Houngbo and J. T. Hounsou, "Measuring information security: understanding and selecting appropriate metrics," *International Journal of Computer Science and Security (IJCSS),* vol. 9, no. 2, p. 108, 2015.

[92] K. Dempsey *et al.*, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations: National Institute of Standards and Technology Special Publication 800-137.* CreateSpace Independent Publishing Platform, 2012.

[93] R. Von Solms, "Information security management: why standards are important," *Information Management & Computer Security,* vol. 7, no. 1, pp. 50-58, 1999.

[94] D. Mellado, E. Fernández-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer standards & interfaces,* vol. 29, no. 2, pp. 244-253, 2007.

[95] Y. Mahy, M. Ouzzif, and K. Bouragba, "Toward a shared view of IT governance," *International Journal of Innovation, Management and Technology,* vol. 7, no. 4, pp. 125-131, 2016.

[96] G. Mangalaraj, A. Singh, and A. Taneja, "IT Governance Frameworks and COBIT-A Literature Review," *Twentieth Americas Conference on Information Systems,* pp. 1-10, 2014.

[97] Y. Bartens, S. De Haes, Y. Lamoen, F. Schulte, and S. Voss, "On the way to a minimum baseline in IT governance: using expert views for selective implementation of COBIT 5," in *48th Hawaii International Conference on System Sciences (HICSS)*, pp. 4554-4563, 2015.

[98] A. Preittigun, W. Chantatub, and S. Vatanasakdakul, "A Comparison between IT Governance Research and Concepts in COBIT 5," *International Journal of Research in Management & Technology,* vol. 2, no. 6, pp. 581-590, 2012.

[99] D. Oliver and J. Lainhart, "COBIT 5: Adding value through effective GEIT," *EDPACS,* vol. 46, no. 3, pp. 1-12, 2012.

[100] N. Ahmad and Z. M. Shamsudin, "Systematic Approach to Successful Implementation of ITIL," *Procedia Computer Science,* vol. 17, pp. 237-244, 2013.

[101] P. Yamakawa, C. Obregón Noriega, A. Novoa Linares, and W. Vega Ramírez, "Improving ITIL compliance using change management practices: a finance sector case study," *Business Process Management Journal,* vol. 18, no. 6, pp. 1020-1035, 2012.

[102] L. Lema, J. A. Calvo-Manzano, R. Colomo-Palacios, and M. Arcilla, "ITIL in small to medium-sized enterprises software companies: towards an implementation sequence," *Journal of Software: Evolution and Process,* vol. 27, no. 8, pp. 528-538, 2015.

[103] K. Suhairi and F. L. Gaol, "The Measurement of Optimization Performance of Managed Service Division with ITIL Framework using Statistical Process Control," *Journal of Networks,* vol. 8, no. 3, pp. 518-529, 2013.

[104] L. Kralik, R. Senkerik, and R. Jasek, "Proposal Of Evaluation Criteria For Free And Open Source Tools For Modelling And Support Of IT Service Management According To ITIL," in *29th European Conference on Modelling and Simulation (ECMS)*, pp. 537-542, 2015.

[105] A. El Yamami, S. Ahriz, K. Mansouri, M. Qbadou, and E. Illoussamen, "Developing an Assessment Tool of ITIL Implementation in Small Scale Environments," *International Journal of Advanced Computer Science and Applications,* vol. 8, no. 9, pp. 183-190, 2017.

[106] I. Ranggadara and H. Prastiawan, "Strategy Implementing Continual Service Improvement with ITIL Framework at PT. Anabatic Technologies Tbk," *International Research Journal of Computer Science,* vol. 5, no. 02, pp. 70-76, 2018.

[107] R. Jašek, L. Králík, and J. Nožička, "ITIL®–General overview," in *AIP Conference Proceedings*, pp. 1-4, 2015.

[108] B. Verlaine, I. Jureta, and S. Faulkner, "Towards the Alignment of a Detailed Service-Oriented Design and Development Methodology with ITIL v. 3," in *International Conference on Exploring Services Science*, pp. 123-138, 2015.

[109] A. Hakemi, S. R. Jeong, I. Ghani, and M. G. Sanaei, "Enhancement of VECTOR Method by Adapting OCTAVE for Risk Analysis in Legacy System Migration," *KSII Transactions on Internet and Information Systems (TIIS),* vol. 8, no. 6, pp. 2118-2138, 2014.

[110] U. K. Singh and C. Joshi, "Information Security Risk Management Framework for University Computing Environment," *IJ Network Security,* vol. 19, no. 5, pp. 742-751, 2017.

[111] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," *Pittsburgh, PA, Carnegie Mellon University,* 2003.

[112] M. I. Javaid and M. M. W. Iqbal, "A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk

management in small/medium enterprises (SME)," in *International Conference on Communication Technologies (ComTech)*, pp. 78-90, 2017.

[113] C. J. Alberts, A. J. Dorofee, and J. H. Allen, "OCTAVE Catalog of Practices, Version 2.0," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2001.

[114] O. Gadyatskaya, K. Labunets, and F. Paci, "Towards empirical evaluation of automated risk assessment methods," in *International Conference on Risks and Security of Internet and Systems*, pp. 77-86, 2016.

[115] V. Agrawal, "A Comparative Study on Information Security Risk Analysis Methods," *Journal of Computers,* vol. 12, no. 1, pp. 57-67, 2017.

[116] J. E. Mbowe, I. Zlotnikova, S. S. Msanjila, and G. S. Oreku, "A conceptual framework for threat assessment based on organization's information security policy," *Journal of Information Security,* vol. 5, no. 4, pp. 166-177, 2014.

[117] S. Dashti, P. Giorgini, and E. Paja, "Information Security Risk Management," in *IFIP Working Conference on The Practice of Enterprise Modeling*, pp. 18-33, 2017.

[118] A. Chandrashekhar, Y. Huded, and H. S. Kumar, "Advances in Information security risk practices," *International Journal of Advanced Research in data mining and Cloud computing (IJARDC),* vol. 3, no. 5, pp. 47-51, 2015.

[119] M. Ghazouani, S. Faris, H. Medromi, and A. Sayouti, "Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk," *International Journal of Computer Applications,* vol. 103, no. 8, pp. 36-42, 2014.

[120] M. Coetzee, "Towards a Holistic Information Security Governance Framework for SOA," in *Seventh International Conference on Availability, Reliability and Security (ARES)*, pp. 155-160, 2012.

[121] L. Kauspadiene, A. Cenys, N. Goranin, S. Tjoa, and S. Ramanauskaite, "High-Level Self-Sustaining Information Security Management Framework," *Baltic Journal of Modern Computing,* vol. 5, no. 1, p. 107, 2017.

[122] M. Shariati, F. Bahmani, and F. Shams, "Enterprise information security, a review of architectures and frameworks from interoperability perspective," *Procedia Computer Science,* vol. 3, pp. 537-543, 2011.

[123] C. Magnusson and S.-C. Chou, "Risk and Compliance Management Framework for Outsourced Global Software Development," in *5th IEEE International Conference on Global Software Engineering (ICGSE)*, pp. 228-233, 2010.

[124] S. Van den Bosch, "Designing Secure Enterprise Architectures A comprehensive approach: framework, method, and modelling language," 2014.

[125] M. Phillips, "Using a capability maturity model to derive security requirements," *SANS InfoSec Reading Room, GSEC Practical v1,* pp. 2-29, 2003.

[126] I. Riadi and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance," *International Journal of Computer Applications,* vol. 141, no. 8, 2016.

[127] P. Jacobs, A. Arnab, and B. Irwin, "Classification of security operation centers," in *Information Security for South Africa*, pp. 1-7, 2013.

[128] K. Höne and J. H. P. Eloff, "Information security policy—what do international information security standards say?," *Computers & Security,* vol. 21, no. 5, pp. 402-409, 2002.

[129] V. Arora, "Comparing different information security standards: COBIT v s. ISO 27001," *BSI-Standard 100-1,* 2010.

[130] M. Belcourt, "Outsourcing—The benefits and the risks," *Human resource management review,* vol. 16, no. 2, pp. 269-279, 2006.

[131] S. Abouen, V. Ahmed, and G. Aouad, "Project manager development in the Libyan oil Industry," ed, 2014.

[132] E. Karaman and M. Kurt, "Comparison of project management methodologies: prince 2 versus PMBOK for it projects," *Int. Journal of Applied Sciences and Engineering Research,,* vol. 4, pp. 657-664, 2015.

[133] S. Saad, A. Ibrahim, O. Asma, M. S. Khan, and J. Akhter, "PRINCE2 Methodology: An Innovative Way for Improving Performance of Malaysian

AutomotIve Industry," *The Journal of Technology Management and Technopreneurship (JTMT),* vol. 1, no. 1, pp. 101-116, 2014.

[134] H. Hammouch, H. Medromi, and A. Sayouti, "Toward an intelligent system for project management based on the multi agents systems," in *10th International Conference on Intelligent Systems: Theories and Applications (SITA)*, pp. 1-6, 2015.

[135] S. Ghosh, D. Forrest, T. DiNetta, B. Wolfe, and D. C. Lambert, "Enhance PMBOK® by comparing it with P2M, ICB, PRINCE2, APM and Scrum project management standards," *PM World Today,* vol. 14, no. 1, pp. 1-77, 2012.

[136] C. Thuesen, C. A. Boas, M. V. Thorslund, F. Marmier, S. Grex, and S. Lybecker, "Mapping Best and Emerging Practices of Project Management," in *22nd Nordic Academy of Management Conference (NFF2013). University of Iceland Reykjavík*, 2013.

[137] E. S. Dunne, *Project risk management: Developing a risk framework for translation projects*. Kent State University, 2013.

[138] D. Biggins, "Perspectives on Project Management Methods," 2015.

[139] S. Saad, A. Ibrahim, O. Asma, M. S. Khan, and J. Akhter, "PRINCE2 Methodology: An Innovative Way for Improving Performance of Malaysian Automotive Industry," *The Journal of Technology Management and Technopreneurship (JTMT),* vol. 1, no. 1, pp. 101-116, 2014.

[140] C. Chin, E. Yap, and A. Spowage, "Reviewing leading project management practices," *PM World Today,* vol. 12, no. 11, pp. 1-18, 2010.

[141] C. Thuesen, "Mapping practices of project management–merging top-down and bottom-up perspectives," in *IRNOP 2015 Conference*, 2015.

[142] B. M. Suchopar, "The System of Project Manager Competencies in the IT Organization," 2012.

[143] E. Karaman and M. Kurt, "Comparison of project management methodologies: prince 2 versus PMBOK for it projects," *Int. Journal of Applied Sciences and Engineering Research,* vol. 4, no. 5, pp. 657-664, 2015.

[144] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Symposium on requirements engineering for information security (SREIS)*, pp. 94-102, 2005.

[145] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of security threats in information systems," *Procedia Computer Science,* vol. 32, pp. 489-496, 2014.

[146] S. Gerić and Ž. Hutinski, "Information system security threats classifications," *Journal of Information and Organizational Sciences,* vol. 31, no. 1, pp. 51-61, 2007.

[147] M. Alhabeeb, A. Almuhaideb, P. D. Le, and B. Srinivasan, "Information security threats classification pyramid," *24th International Conference on Advanced Information Networking and Applications Workshops (WAINA),* pp. 208-213, 2010.

[148] M. Brandt, R. Khondoker, R. Marx, and K. Bayarou, "Security Analysis of Software Defined Networking Protocols—OpenFlow, OF-Config and OVSDB," in *The Fifth International Conference on Communications and Electronics (ICCE 2014)*, pp. 23-30, 2014.

[149] A. Marback, H. Do, K. He, S. Kondamarri, and D. Xu, "A threat model-based approach to security testing," *Software: Practice and Experience,* vol. 43, no. 2, pp. 241-258, 2013.

[150] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," *IEEE Symposium on Security and Privacy,* pp. 154-163, 1997.

[151] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow, "A management perspective on risk of security threats to information systems," *Information Technology and Management,* vol. 6, no. 2-3, pp. 203-225, 2005.

[152] PMI, *Project Management Body of Knowledge (PMBOK® GUIDE)*. 2001.

[153] M. L. Smith, J. Erwin, and S. Diaferio, "Role & responsibility charting (RACI)," in *Project Management Forum (PMForum)*, p. 5, 2005.

[154] I. Livshitz, P. Lontsikh, and S. Eliseev, "The optimization method of the integrated management system security audit," in *20th Conference of Open Innovations Association (FRUCT)*, pp. 248-253, 2017.

[155] C. Chin, E. Yap, and A. Spowage, "Reviewing leading project management practices," *PM World Today,* vol. 2, 2010.

[156] V. Chidambaram, "Threat modeling in enterprise architecture integration," *Retrieved March,* vol. 2, no. 4, 2004.

[157] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in *IEEE 10th International Conference on Computer and Information Technology (CIT)*, pp. 1328-1334, 2010.

[158] M. S. Toosarvandani, N. Modiri, and M. Afzali, "The risk assessment and treatment approach in order to provide LAN security based on ISMS standard," *International Journal in Foundations of Computer Science & Technology (IJFCST),* vol. 2, no. 6, pp. 15-36, 2012.

[159] C.-h. Jang, T.-S. KIM, and B. AHN, "Factors that Affect Selection of Information Security Countermeasures," ed, pp. 28-30, 2014.

[160] Q.-J. Yeh and A. J.-T. Chang, "Threats and countermeasures for information system security: A cross-industry study," *Information & Management,* vol. 44, no. 5, pp. 480-491, 2007.

[161] P. Khan and K. A. Quraishi, "Impact of RACI on Delivery and Outcome of Software Development Projects," in *Fourth International Conference on Advanced Computing & Communication Technologies*, pp. 177-184, 2014.

[162] S. Balaji and M. S. Murugaiyan, "Waterfall vs. V-Model vs. Agile: A comparative study on SDLC," *International Journal of Information Technology and Business Management,* vol. 2, no. 1, pp. 26-30, 2012.

[163] P. Serrador and J. K. Pinto, "Does Agile work?—A quantitative analysis of agile project success," *International Journal of Project Management,* vol. 33, no. 5, pp. 1040-1051, 2015.

[164] K. E. Ryan, T. Gandha, M. J. Culbertson, and C. Carlson, "Focus group evidence: Implications for design and analysis," *American Journal of Evaluation,* vol. 35, no. 3, pp. 328-345, 2014.

[165] A. Duarte, L. Veloso, J. Marques, and J. Sebastião, "Site-specific focus groups: analysing learning spaces in situ," *International Journal of Social Research Methodology,* vol. 18, no. 4, pp. 381-398, 2015.

[166] M. Parsons and J. Greenwood, "A guide to the use of focus groups in health care research: Part 1," *Contemporary Nurse,* vol. 9, no. 2, pp. 169-180, 2000.

[167] S. Y. Chyung, K. Roberts, I. Swanson, and A. Hankinson, "Evidence-based survey design: The use of a midpoint on the Likert scale," *Performance Improvement,* vol. 56, no. 10, pp. 15-23, 2017.

[168] S. E. Harpe, "How to analyze Likert and other rating scale data," *Currents in Pharmacy Teaching and Learning,* vol. 7, no. 6, pp. 836-850, 2015.

[169] Z. Zainal, "Case study as a research method," *Jurnal Kemanusiaan,* vol. 4, no. 9, pp. 1-6, 2007.

[170] B. Yazan, "Three approaches to case study methods in education: Yin, Merriam, and Stake," *The Qualitative Report,* vol. 20, no. 2, pp. 134-152, 2015.

[171] N. Hyett, A. Kenny, and V. Dickson-Swift, "Methodology or method? A critical review of qualitative case study reports," *International journal of qualitative studies on health and well-being,* vol. 9, no. 1, pp. 1-14, 2014.

[172] S. Baskarada, "Qualitative case study guidelines," *The Qualitative Report,* vol. 19, no. 40, pp. 1-25, 2014.

[173] P. Twining, R. S. Heller, M. Nussbaum, and C.-C. Tsai, "Some guidance on conducting and reporting qualitative studies," vol. 106, ed. Computers & Education, pp. A1-A9, 2017.

[174] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," *Empirical software engineering,* vol. 14, no. 2, pp. 131-164, 2009.

Appendix A Focus Group and Questionnaire

Data Confidentiality

The identity of the participants will be kept anonymous in this research. The data collected will be employed solely for improving the OSCR and for statistical analysis. The participants' names will not be mentioned in any of the research documents. By signing this consent statement you are indicating that you have understood the information supplied to you about participation in the research project and you agree to participate. This does not affect your legal rights or release the investigators, sponsors, or involved institutions from their legal and professional responsibilities. You may decline to answer certain items or questions in the focus group or questionnaires. You may withdraw from the study at any time without specifying a reason, with no penalty. It is important that you continue to feel fully informed about participation, therefore if at any time you have any questions you would like to ask, or you wish to seek clarification on any points, please contact the researcher.

Consent Statement:

I have read the above information and I confirm that I am 18-year old or above. I consent to participate in this evaluation.

Participant Name ……Date: …….

Participant Signature …….

Framework Units & Phases Evaluation (Questionnaire)

1- *The Initiating Phase Units (Project Unit, Stakeholders Unit, and Potential Security Risks Unit) in relation to managing the security and compliance risks of outsourced IT projects are:*
O Not useful *O Somewhat Useful* *O Useful* *O Very useful*
Comments: ----------

2- *The Initiating Phase of the OSCR framework (tick where appropriate):*

□ *covers all required security aspects in this phase.*

□ *covers most of the required security aspects in this phase.*

□ *misses required units: (please comment)*

□ *covers unnecessary units: (please comment)*

3- *The Planning Phase Units (Security Requirements Unit, Assets Unit, Threat Classification Unit, Risk Assessment Unit, Security Controls Unit, Roles And Responsibilities Unit, Risks Repository Unit, And Security Plans Unit) in terms of security risks management of outsourced IT projects are:*

O Not useful O Somewhat Useful O Useful O Very useful

Comments: ----------

4- *The Planning Phase of the OSCR framework (tick where appropriate):*

□ *covers all required security aspects in this phase.*

□ *covers most of the required security aspects in this phase.*

□ *misses required units: (please comment)*

□ *covers unnecessary units: (please comment)*

5- *The Executing Phase Units (Performance Unit, Security Issues Unit, Change Requests Unit, And Security Deliverables Unit) in terms of security risks management of outsourced IT projects are:*

O Not useful O Somewhat Useful O Useful O Very useful

Comments: ----------

6- *The Executing Phase of the OSCR framework (tick where appropriate):*

□ *covers all required security aspects in this phase.*

□ *covers most of the required security aspects in this phase.*

□ *misses required units: (please comment)*

□ *covers unnecessary units: (please comment)*

7- *The Monitoring and Controlling Phase Units (Evaluation Unit, Auditing Unit, Issue Resolution Unit, Change Approval Unit, And Deliverables Approval Unit) in relation to managing security risks in outsourcing context are:*

O Not useful O Somewhat Useful O Useful O Very useful

Comments: ----------

8- *The Monitoring and Controlling Phase of the OSCR framework (tick where appropriate):*

□ *covers all required security aspects in this phase.*

□ *covers most of the required security aspects in this phase.*

□ *misses required units: (please comment)*

□ *covers unnecessary units: (please comment)*

9- *The Closing Phase Units (Auditing Unit, Lessons Learned Unit, And Closure Unit) in relation to managing security risks in outsourcing context are:*

O Not useful O Somewhat Useful O Useful O Very useful

Comments: ----------

10- *The Closing Phase of the OSCR framework (tick where appropriate):*

□ *covers all required security aspects in this phase.*

□ *covers most of the required security aspects in this phase.*

□ *misses required units: (please comment)*

□ *covers unnecessary units: (please comment)*

OSCR Framework Overall Evaluation (Questionnaire)

1- *The main architecture of the OSCR framework is:*

□ *Understandable.*

□ *Simple and easy to use.*

□ *Difficult.*

□ *Requires some improvements (please comment):*

2- Utilising project phases in managing security risks of outsourced IT projects is:

O Not useful O Somewhat Useful O Useful O Very useful

Comments: ----------

3- To what extent do you agree with the statement that adopting the Plan-Do-Check-Act (PDCA) model in managing the security risks of outsourced projects improves the framework's flexibility?

O Disagree O Neutral O Somewhat Agree O Agree

Comments: ----------

4- Do you agree with the statement that the OSCR framework provides a systematic and comprehensive approach for managing the security and compliance risks of outsourced IT projects?

O Disagree O Neutral O Somewhat Agree O Agree

Comments: ----------

5- The proposed threat classification approach provides an effective and useful way for identifying security threats in outsourcing contexts.

O Disagree O Neutral O Somewhat Agree O Agree

Comments: ----------

6- To what extent do you agree that the OSCR framework can be applied to any outsourced IT projects regardless of project size, cost, or any other constraints?

O Disagree O Neutral O Somewhat Agree O Agree

Comments: ----------

Appendix B Case Study

Data Confidentiality

Confidentiality and participant anonymity will be strictly maintained. All information gathered will be used for improving the OSCR and statistical analysis only and no names or other identifying characteristics will be stated in the final or any other reports. Your signature on consent statement indicates that you have understood to your satisfaction the information regarding participation in the research project and agree to take part as a participant. In no way does this waive you legal rights nor release the investigators, sponsors, or involved institutions from their legal and professional responsibilities. You are free to not answer specific items or questions in the focus group or questionnaires. You are free to withdraw from the study at any time without penalty. Your continued participation should be as informed as your initial consent, so you should feel free to ask for clarification or new information throughout your participation. If you have further questions concerning matters related to this research, please contact the researcher.

Consent Statement

I hereby confirm that I have read the above information and I am 18-year old or above. I consent to participate in this evaluation.

Participant Name ……Date: …….

Participant Signature …….

OSCR Framework Guidelines

The OSCR framework is designed to manage the security and compliance risks of outsourced IT projects effectively. It utilises project phases (Initiating, Execution, Monitoring and Controlling, and Closing) and the Plan-Do-Check-Act (PDCA) model, as shown in Figure B-1. In the PDCA model, the Plan stage involves planning how to deliver the desired outputs of the project that meet the

client's business needs. This stage reflects exactly what the planning phase does in the OSCR framework. The Do stage is designed to allow carrying out the plans developed in the previous stage. The Execution phase in our framework represents this stage of the PDCA model. The Check stage involves evaluating performance in the Do stage. The Act stage is used to propose new changes if the performance evaluation in the previous stage shows that the plans developed in the plan stage will not achieve the desired outputs. Those two stages are represented by Monitoring and Controlling Phase in our OSCR framework.

The OSCR framework also uses a hybrid threat classification approach that is designed for the outsourcing context, in which environments are less stable and more systems are integrated. The threat classification approach considers threats from different perspectives such as external threats, provider threats, client threats, and physical and environmental threats. The following sub-sections explain the framework phases in more details.

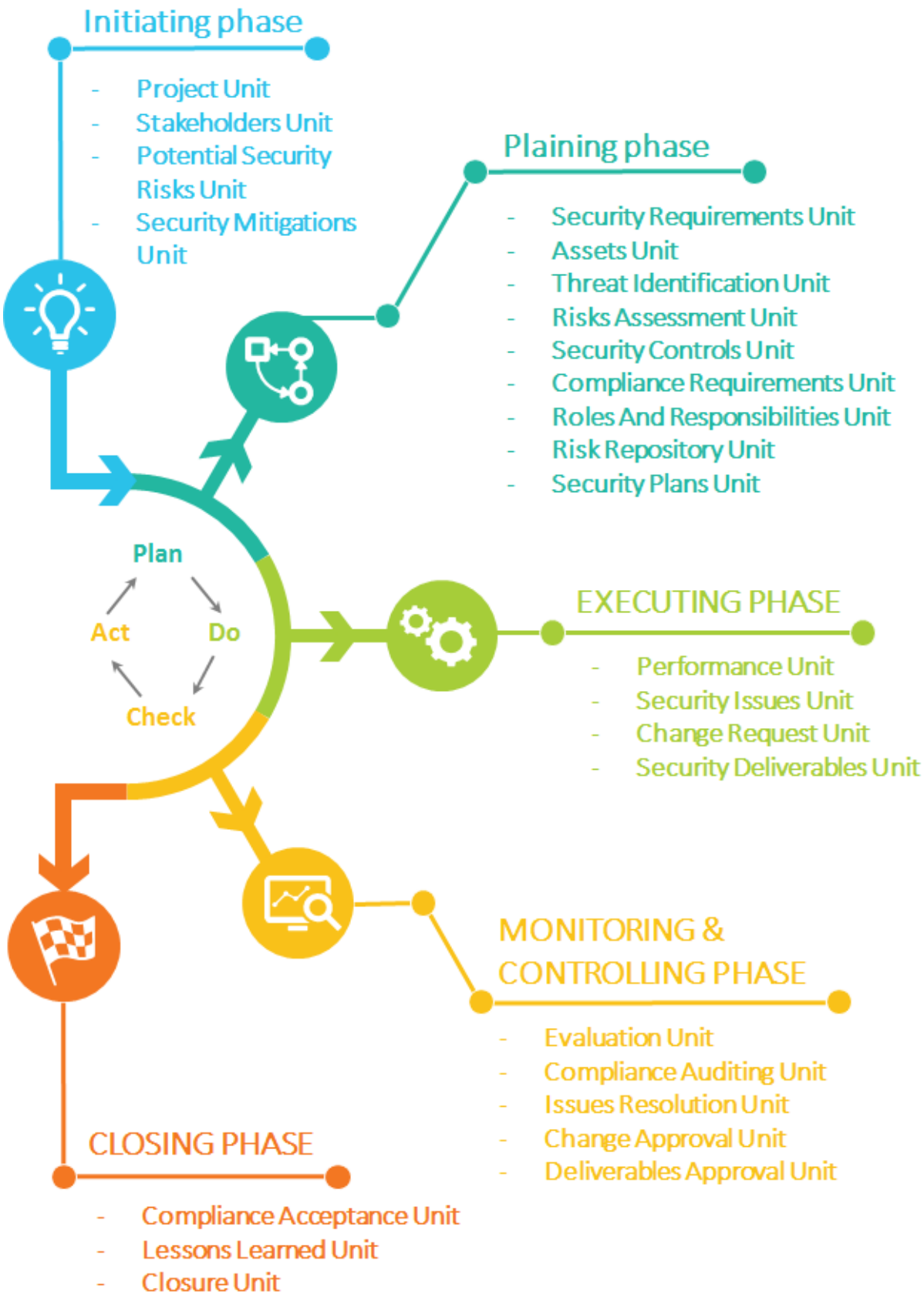

Figure 0.1: OSCR Framework

Initiating Phase

The aim of this phase is to establish the project's unique details, and identify major project stakeholders and potential security risks to which the project might be exposed, as well as security controls that will be used to mitigate the potential security risks. The client is responsible for this phase, as no provider has yet been selected. This phase achieves its objectives through the following units:

- **Project Unit**

Designed to handle (create, update) essential project data such as project ID, name, code…etc. Please use the following table for this purpose.

Table B-1: Project Essential Data

Project ID		Project Code	
Project Name			
Project Type			
Project Start Date			
Project End Date			
Project Duration			
Project Owner			
Project Provider			
Project Manager			
Project Cost			

- **Stakeholders' Unit**

The aim of this unit is to identify all project stakeholders and their roles and responsibilities in the project. Please use the following table for this purpose.

Table B-2: Stakeholders Data

Project ID		Project Code	
Stakeholders' Data			
Stakeholder Name	Stakeholder Type	Stakeholder Role	

- **Potential Security Risks Unit**

The aim of this unit is to identify potential security risks that might take place while executing the project. This allows decision makers to take the right decision about whether to outsource or not. Please use the following table for this purpose.

Table B-3: Potential Security Risks

Project ID		Project Code	
Potential Security Risks			
RISK ID	Risk Description		
1			
2			
3			

- **Security Mitigations Unit**

Designed to propose and implement security controls (countermeasures) that will be used to mitigate the potential security risks. Please use the following table for this purpose.

Table B-4: Security Countermeasures

Project ID		Project Code	
Risk ID	Countermeasure Type	Security Countermeasures	
R1			
R2			
R3			

Planning Phase

The planning phase is the core part of this framework. It corresponds to the plan stage of the PDCA model. The planning phase aims are achieved in units as follows:

- **Security Requirements Unit**

The project security requirements are documented and signed off by the client and the provider through this unit. Please use the following table for this purpose.

Table B-5: Security Requirements

Project ID		Project Code	
Security Requirements			
Requirement ID	Requirement Description		
RQ-1			
RQ-2			
RQ-3			

- **Assets Unit**

All project assets are identified and categorised (hardware, software, information, network, or human) through this unit. It answers the question about what should be protected. If the project affects any organisation's assets, then they should be identified and categorised as well. Please use the following table for this purpose.

Table B-6: Project Assets

Project ID		Project Code	
Project Assets			
Asset Type	Asset ID	Asset description	
Hardware			

Project ID		Project Code	
Project Assets			
Asset Type	Asset ID	Asset description	
Software			
Network			
Information			

- **Threat Classification Unit**

A hybrid threat classification approach is designed to be capable of identifying the wide range of potential security threats that might occur during the project execution. In another words, it identifies what to protect from. This threat classification approach uses six criteria:

- Threat Source: it represents the origin of the threat, which can be external threats, client threats, provider threats, or environmental and physical threats.
- Threat agent: the agent that causes the threat. This can be technical, human, or organisational.
- Asset type: the type of the asset impacted by this threat, such as networks, software, hardware, information.
- Threat intention: the type of human behaviour that caused the threat. It can be accidental or intentional.
- Environmental and physical threat type: the type of environmental and physical threat. It can be controlled or uncontrolled.
- Threat impact: the result of the threat when it occurs. This can be any breach in confidentiality, integrity, or availability.

Please use the following tables for this purpose.

Table B-7: External Threats

Project ID			**Project Code**	
External Threats				**Impact**
	Software:			C-I-A
	Hardware:			
	Network:			
	Information:			
Human	Accidental:			
	Intentional:			

Table B-8: Provider Threats

Project ID			**Project Code**	
Provider threats				**Impact**
Technical				C-I-A
	Software:			
	Hardware:			
	Network:			
	Information:			
Human	Accidental:			
	Intentional:			
Organisational				

Table B-9: Client Threats

Project ID			**Project Code**	
Client threats				**Impact**
	Software:			C-I-A
	Hardware:			
	Network:			
	Information:			
Human	Accidental:			
	Intentional:			
Organisational				

Table B-10: Environmental & Physical Threats

Project ID		**Project Code**	
Environmental & Physical Threats			**Impact**
Controlled:			C-I-A
Non-Controlled:			

- **Risk Assessment Unit**

The ultimate aim of this unit is to estimate and prioritise the impact of the potential security risk on project assets. The risk assessment unit has five steps: vulnerabilities identification, risk likelihood determination, risk magnitude determination, risk estimation, and risk prioritisation.

These five steps are described as follows:

- Vulnerabilities identification: it is essential to identify all vulnerabilities that might be used by threat sources identified in the previous section to calculate risks exposure.

- Risk likelihood determination: the OSCR framework utilises NIST SP 800-30 (Guide for Conducting Risk Assessments)[19], and divides the likelihood of the risk into five number ranges (0-20, 21-40, 41-60, 61-80, and 81-100). These ranges represent five level values (very low, low, moderate, high, and very high) respectively. Table B-11 shows the threat likelihoods values and their description for the OSCR framework.

Table B-11: Threat likelihoods

Qualitative Values	Semi-Quantitative Values %	Description
Very High	81-100	Almost certain that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).
High	61-80	High likely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).
Moderate	41-60	Somewhat likely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).
Low	21-40	Unlikely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).
Very Low	0-20	High unlikely that threat will be initiated by threat sources (external, provider, client, or environmental and physical threats).

- Risk magnitude determination: In a similar way to the risk likelihood categories, the magnitude or impact of the risk is divided into five number categories (1, 2, 3, 4, and 5), which represent five level values (minor, moderate, major, critical, and severe) respectively. Table B-12 shows the threat impact values and their description for the OSCR framework.

Table B-12: Threat Impacts (magnitudes)

Qualitative Values	Semi-Quantitative Values	Description
Severe	5	Multiple severe or catastrophic impacts on the project, or organisation assets if the threat occurs.
critical	4	Severe or catastrophic impact on the project, or organisation assets if the threat occurs.
Major	3	Serious impact on the project, or organisation assets if the threat occurs.
Moderate	2	Limited impact on the project, or organisation assets if the threat occurs.
Minor	1	Negligible impact on the project, or organisation assets if the threat occurs.

- Risk estimation: In the OSCR framework, we will use a semi-quantitative method to estimate the security risks of outsourced IT projects as shown in Table B-11 and Table B-12. This will allow decision makers to understand risk assessment results easily and also help risk assessors to assess risks more accurately and to interpret them to an understood value (e.g. 80 interpreted to high) We will also use the ordinary risk exposure (RE) equation, which has been used in many risk assessment analyses for risk estimation. In the RE equation, the risk exposure is the result of the likelihood multiplied by the magnitude or the impact of the risk. The RE equation is used as follows:

$$RE = likelihood * magnitude$$

Following the above guidance and explanation, security risks can be estimated easily using the risk exposure equation. Please use the following table for this purpose.

Table B-13: Risk Estimation

Project ID		Project Code	
Risk ID			
Asset Type			
Asset ID			
Asset Name			
Threat			
Threat Source			
Vulnerability			
Risk Likelihood			
Magnitude			
Risk Exposure			

- Risk prioritisation: the last step in this unit but not the least is intended to prioritise the risks estimated in the previous step. The aim of this step is to allow project teams to concentrate first on risks that impose higher impacts on confidentiality, integrity, and availability of project assets. Please use the following table for this purpose.

Table B-14: Risk Prioritisation

Project ID		Project Code	
Risk ID	Threat Source	Risk Description	RE
R1			
R2			
R3			

- **Security Controls Unit**

Through this unit, security controls or countermeasures that can mitigate identified security risks are selected. Countermeasures determine how to protect project or organisation assets. Countermeasures are categorised in this framework into technical, human, or organisational. Please use the following table for this purpose.

Table B-15: Security Countermeasures

Project ID		Project Code	
Risk ID	Countermeasure Type	Security Countermeasures	
R1			
R2			
R3			

- **Compliance Requirements Unit**

Designed to identify compliance requirements that will be audited by the project steering committee.

- **Roles and Responsibilities Unit**

The aim of this unit is to assign security activities to project teams using a clear method that helps prevent any ambiguities between the project teams. We use a role-based and name-based version of the responsible, accountable, consult, and inform method (RACI) for assigning the roles and responsibilities of project security activities. Please use the following table or a similar one for this purpose.

Table B-16: Roles and Responsibilities

Project ID	1		Project Code		API/PNR
Security Activity	Project Owner	Project Manager	Business Analyst	Security Architect	Development Team
Security requirements					
Project assets					
Threat classification					

- **Risk Repository Unit**

This unit contains all of the thus-far identified project security risks. Any risk that has been logged into the risk repository unit should have sufficient

information about the risk such as risk ID, description, impact, asset name, and so on. Please use the following table for this purpose.

Table B-17: Risk Repository Entry

Project ID		Project Code	
Risk ID			
Asset Type			
Asset ID			
Asset Name			
Threat			
Threat Source			
Vulnerability			
Risk Likelihood			
Magnitude			
Risk Exposure			
Risk Description			
Impact on Security			
Security Controls			

- **Security Plans Unit**

This unit is responsible for developing security plans that will be used to achieve the project's security goals and contribute to building a secure and protected environment such as an incident management plan, business continuity management plan, and so on.

Executing Phase

This phase, which represents the Do stage of the PDCA model, achieves its objectives through the following units:

- **Performance Unit**

Prepare and submit security performance reports. These reports are reviewed and signed off by the project steering committee in the next phase.

- **Security Issues Unit**

Record any security issues that might be experienced during the project's execution.

- **Change Requests Unit**

If there is any need to change any security plan or control, the change is raised through this unit.

- **Security Deliverables Unit**

Ensure that security deliverables are submitted on time to avoid any delay, which might lead to penalties.

Monitoring and Controlling Phase

This phase, which represents the Check and Act stages of the PDCA model, achieves its objectives through the following units:

- **Evaluation Unit**

The security performance reports are reviewed and assessed. Based on this review, the project steering committee may propose improvements that help to achieve the project's security goals in an effective and efficient way. If the performance is good and there is no need for any improvement, then the steering committee signs off the existing performance reports.

- **Compliance Auditing Unit**

This unit is designed to enforce compliance with the compliance requirements to reduce any security violations.

- **Issues Resolution Unit**

Security issues that might be experienced during the project execution are resolved. Security issues resolution might be beyond the ability of the project

manager, and therefore intervention by the project steering committee might help in their resolution.

- **Change Approval Unit**

The project steering committee analyses security changes and assesses their potential impact on different aspects such as the project budget and schedule. If these changes can be tolerated by both parties, then they approve them.

- **Deliverables Approval Unit**

The security deliverables that have been achieved so far are reviewed and approved, or rejected.

Closing Phase

This phase achieves its objectives through the following units:

- **Compliance Acceptance Unit**

Designed to accept or reject the project's compliance with the requirements identified in the planning phase based on the assessment of the compliance carried out by the project steering committee in the Monitoring and Controlling phase.

- **Lessons Learned Unit**

Document all security lessons learned for future use.

- **Closure Unit**

Issue the provider with the project closure certificate and officially close the project.

OSCR Framework Evaluation and Improvements

Having applied the framework to your outsourced IT project, please provide us with your feedback by answering the following questions:

1- *What is the current security framework or standard that you use for managing security risks for outsourcing?*

2- *In comparison with the current security or framework that you use, how do you rate the OSCR framework?*

 Provides better management for security risks of outsourced IT projects in all phases.

 Provides better management for security risks in some phases. (Please comment): ---

 Same as the current security framework or standard that you use.

 Provides lower management for security risks of outsourced IT projects.

3- *What are the issues that you think exist in the OSCR framework?*

4- *What improvements could be made to the OSCR framework in order to increase its ability to manage the security risks of outsourcing more effectively?*
