UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Gayanjalie Dissanayake

A Comparison of Security Risk Analysis in the In-house IT Infrastructure and Cloud Infrastructure for the Payment Gateway System

Master's Thesis (30 ECTS)

Supervisor(s): Hayretdin Bahsi PhD
Raimundas Matulevičius PhD

Tartu 2019

A Comparison of Security Risk Analysis in the In-house IT Infrastructure and Cloud Infrastructure for the Payment Gateway System

Abstract:

In-house infrastructures are migrated to the cloud owing to the enhanced technical management capabilities, technical advancement as well as the flexibility and cost-effective options offered by the cloud. Moreover, an enterprise architecture changes when the systems are moved into a different infrastructure. Due to such infrastructural changes, security risks can increase or decrease, while new risks can be introduced and some risks can be eliminated. Asset identification for risk analysis based only on business process modelling lacks the integration and representation of the interrelationship between IT infrastructure and business processes. Hence, certain information system (IS) assets can be neglected in the risk analysis. When analysing the security risk of two infrastructures, enterprise architectural differences need to be captured, since unidentified IS assets could be vulnerable and pose a security risk to the concerned organisation.

In this thesis, assets are identified via architectural modelling to perform risk analysis. Furthermore, models present the differences pertaining to IS assets within in-house infrastructure and cloud infrastructure, in addition to the mapping to corresponding business processes. The STRIDE-based threat modelling is employed to determine the security risks concerning IS assets derived from enterprise architecture.

To elaborate, this study will introduce a procedure that will help organisations identify IS asset changes of two different infrastructures and capture security risk changes. Moreover, architectural modelling applied in this research will illustrate the differences regarding IS assets and present the way in which business processes are mapped to technology components. Subsequently, a threat modelling method employed will provide a structural way to identify threats to the systems. The changes incorporated concerning the security risks will further present the security risk gap regarding in-house infrastructure and cloud infrastructure. Additionally, the validation of this approach is performed by domain experts. The enterprise architecture modelled in this thesis is based on a case study dealing with a payment gateway system used in the North Europe.

Keywords:

Security risk analysis, ArchiMate, ISSRM, Enterprise architecture, Cloud infrastructure, Threat modelling, Payment gateway system, BPMN

CERCS:

T120 - Systems engineering, computer technology

Maksekanali turvariskide võrdlev analüüs põhinedes IT infrastruktuurile ja pilve infrastruktuurile

Lühikokkuvõte:

Infrastruktuuri lahendused viiakse pilve tänu paremale juhtimisvõimekusele, seadmete tehnilisele arengule ning pilve lahenduste paindlikkusele ja kuluefektiivsetele võimalustele. Seetõttu muutub ettevõtte arhitektuur, kui süsteemid viiakse uude infrastruktuuri. Selliste muutuste tõttu võivad turvariskid suureneda või väheneda, avalduda uued riskid või suudetakse kõrvaldada mõned olemasolevad riskid. Ainult äriprotsesside modelleerimisele tugineva riskianalüüsi puhul, kus tuvastatakse ettevõtte varade väärtus, puudub IT-infrastruktuuri ja äriprotsesside omavahelise seose esindamine. Seega võib riskianalüüsis teatud infosüsteemi (IS) varasid hoopis eirata. Kahe infrastruktuuri turvariskide analüüsimisel tuleb arvestada ettevõtte arhitektuurilisi erinevusi, sest identifitseerimata IS varad võivad olla haavatavad ja kujutada ohtu käsitletavale organisatsioonile.

Käesolevas töös tuvastatakse arhitektuuri modelleerimise kaudu varad, mis on vajalikud riskianalüüsi tegemiseks. Koostatud mudelid näitavad erinevusi, mis on seotud IS varadega organisatsiooni sisemise infrastruktuuri ja pilves vahel. Organisatsiooni arhitektuurist tulenevate IS varadega seotud turvariskide kindlaksmääramisel kasutatakse STRIDE taksonoomia põhist ohu modelleerimist.

Selles uurimistöös esitletakse protseduuri, mis aitab organisatsioonidel tuvastada kahe infrastruktuuri IS varade muutusi ja mõista turvariskide erinevusi. Käesolevas uurimistöös kasutatud arhitektuuri modelleerimine illustreerib IS varade erinevusi ja näitab, kuidas äriprotsesse saab kaardistada tehnoloogia komponentidega. Seejärel võimaldab ohu modelleerimine struktuurselt määrata süsteemi ohtusid. Vastavad turvariskid kategoriseeritakse põhinedes uue infrastruktuuri olemasolule. Riskidega seotud muutused toovad esile ettevõtte sisemise infrastruktuuri ja pilve infrastruktuuri vahe. Selline lähenemisviis on kinnitatud ekspertide poolt. Käesolev uurimistöö põhineb juhtumiuuringul, mis käsitleb Põhja-Euroopas kasutatavat maksekanali süsteemi.

Võtmesõnad:

Riskianalüüs, ArchiMate, ISSRM, ettevõtlusarhitektuur, turvariskide juhtimine, pilvinfrastruktuur, Ohu modelleerimine, Maksevõrgu süsteem, BPMN

CERCS:

T120 – Süsteemitehnoloogia, arvutitehnoloogia

Contents

Table of Figures

List of Tables

Acronyms and Abbreviations

ISSRM	Information System Security Risk Management
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privileges
PCI DSS	Payment Card Industry Data Security Standard
NIST	National Institute of Standards and Technology
MEHARI	Method for Harmonized Analysis of Risk
IS	Information Systems
EA	Enterprise Architecture
RM	Risk Management
RA	Risk Analysis
CIA	Confidentiality, Integrity, Availability
PSP	Payment Service Provider
ISO/IEC	International Organisation for Standardisation and the International Electrotechnical Commission
BPMN	Business Process Model and Notation
SP	Spoofing
TA	Tampering
RE	Repudiation
IND	Information Disclosure
DS	Denial of Service
EP	Elevation of Privilege
WAF	Web Application Firewall
IaaS	Infrastructure as a Service
SaaS	Software as a Service
PaaS	Platform as a Service.

1 Introduction

Cloud has become a choice, than a trend of top-level decision makers for new and existing IT infrastructures. Migrating in-house infrastructure to cloud infrastructure have advantages such as the use of high-end latest technologies, flexibility, management facilities and be competitive in the dynamic world [1]. With the evolvement of cloud technology, security has become a cloud challenge [2]. The possibilities of the third parties gaining unauthorised access to confidential resources, account hijacking, denial of service and malicious insider attacks are risks on cloud environments. But despite these fears, there is still a hype around cloud computing. According to Gartner predictions [3], 80% of in-house enterprise data centres will close down by 2025 because of the cloud. The fourteenth annual worldwide infrastructure security report by Netscout [4], shows that 49% of enterprise applications are already in the cloud.

Cloud Infrastructure related security risks can be different from an in-house data centre because of the cloud enterprise architectures. Therefore, a risk analysis (RA) conducted to a business process in an in-house infrastructure will not apply to the cloud even though the business process remains constant. These changes to system assets pose threats and therefore security risks can either remain, eliminate or initiate when a cloud migration happens. Information system asset identification based only on business process modelling fails to capture the enterprise architectural changes of a system before and after migration. Assets need to be identified before conducting a RA in any given context. Information system assets are the assets that support business assets and needs to be protected from threats [5]. In organisations, a non-technical person conducts the business process analysis. Therefore, the business process focused analysis lacks the reflection of all the information system assets which support the business assets. Furthermore, the mapping between the business process and corresponding infrastructure are absent and isolated.

This thesis is focused on proposing a procedure to capture and compare security risk differences due to infrastructure change that happens when a payment gateway system is migrated. The study provides a model-driven approach which can identify the changes to system assets when infrastructure changes and the interdependencies to business processes. Enterprise architecture modelling is used to identify the architectural differences between in-house and cloud infrastructure. The approach reflects the interrelationships and interdependencies of business and system assets which helps to find what assets will have an impact due to a security risk. Information Systems Security Risk Management (ISSRM) is used as the RA method to identify the security risks of in-house and cloud infrastructure [5]. The differences of the security risks identified in the study are considered as the security risk gap in the work. This thesis is a case study based on a payment gateway system. The organisation of the payment gateway system requires to know what security risks will change due to cloud migration. Unidentified information system assets pose threats to the organisation and make security risk analysis incomplete. The business process in the study will remain constant, and therefore the changes to the infrastructure need to be focused on eliciting information system assets from in-house and cloud architecture.

Payment gateway system in in-house infrastructure is hosted in a non-virtualized environment while the cloud model is based on virtualization technology. Due to privacy issues disclosing the payment gateway name is prohibited. Therefore going forward payment gateway name is referred to as “PayGate”.

The main research question of the study is,

What procedure can be used to find differences of security risks in the in-house infrastructure and cloud infrastructure?

This main research question has three sub-research questions,

RQ 1: What are the architectural differences between in-house infrastructure and cloud infrastructure?

RQ 2: What are the business assets and supporting information system assets?

RQ 3: What security risks change when a payment gateway system migrates from in in-house to cloud infrastructures?

This thesis will contribute to the organisations planning to migrate their payment gateways to cloud infrastructure by the STRIDE-based security risk gap analysis. The procedure illustrates how to capture information system assets using enterprise architecture. The work extracts a business asset from the payment transaction process and present the interrelationship to information systems using ArchiMate. Afterwards, threat modelling based on the STRIDE is performed to find out threats in in-house and cloud infrastructure. The following are identified after threat analysis;

1. The security risks in in-house architecture.
2. The security risks in cloud architecture.
3. The security risks differences in in-house architecture and cloud architecture.

The findings presented in the work is validated by experts in the company to find the correctness of the models and usefulness of the approach to do a comparison in the enterprise. The external opinion is taken to find the usefulness of such an approach in the industry.

This study consists of 7 chapters including the introduction and conclusion. Chapter 1 presents the introduction to the problem, motivation of the research and scope of the study. Reports were analysed to find out the statistics and past trends to prove the importance. Chapter 2 consists of the methods and modelling languages used in the study providing previous related work and presenting justification for the method chosen. Chapter 3 gives an introduction of payment gateway types and an overview of the infrastructures used in the study. Also, it presents the enterprise architecture of in-house and cloud infrastructure to identify the context and the relationship of business assets and supporting assets using Enterprise Architecture (EA) modelling. Chapter 4 focuses on eliciting assets and presenting security objectives of business assets. Chapter 5 concentrates on finding threats to information system assets in in-house infrastructure and cloud infrastructure using the STRIDE threat modelling method. Furthermore, how risks will differentiate based on infrastructure migration will be discussed. Chapter 6 evaluate the correctness and the usefulness of the approach used to find the security risk gap between infrastructures based on the expert's ideas. Chapter 7 concludes the research and provides limitations of the study. Suggestion for future work is presented as a continuation of the work.

2 Literature Review and Background

This chapter provides the theoretical background of security risk management methods, standards, notations, threat modelling techniques and previous research work that was conducted. Furthermore, this chapter explains what approaches are used to compare security risks that will diverse due to the cloud infrastructural migration by using a payment gateway as a case study.

2.1 Security Risk Management Standards

Security risk management standards have been implemented as a guideline to manage security risks in information systems. There are various number of standards that have been newly created and merged from existing standards. Since this research is based on conducting a risk analysis for a payment gateway in Germany, IT-Grundschutz, PCI DSS and company-specific requirements are discussed apart from the industry leading standards such as ISO/IEC 27xx and NIST as seen in figure 1.

National Institute of Standards and Technology (NIST) in the US has published several standards related to security risk management and assessment in information technology systems. NIST special publication 800-30 is a guide for conducting a risk analysis which explains from assignment preparation to assessment maintenance as well as how the risk assessment and risk management of different organisations will correlate to each other [6]. NIST SP 800-39 is a publication which represents organisation, business process and system level aspects when managing information security risk and it supports the steps described in the risk management framework. In addition, NIST SP 800-53 and NIST SP 800-37 also describe the risk management process and privacy related to cloud [7].

According to the PCI security standards council, Payment Card Industry Data Security Standard (PCI DSS) is a worldwide standard for any entity that store, process and transmit cardholder data [8]. The PCI DSS standard indicates and address technical and operational aspects. Payment gateway system which is the study based on needs to be PCI compliant because it manages credit card details. The standard consists of twelve requirements, and it is essential to have a continuous assessment for maintenance. Inadequacy to fulfil the requirement can lead to monetary losses and sensitive data breaches leaving the organisation a bad reputation.

The ISO/IEC 2700x family consists of several standards related to information security management systems (ISMS) [9]. The ISO/IEC 27005 standard is specifically designed to assist information security risk management approaches, and it is aligned with the basic concepts defined in ISO/IEC 27001 [10]. The company of the payment gateway system in the case study is maintaining ISO/IEC 27005: 2011 standard.

IT-Grundschutz is a standard developed in Germany which provides a best practice approach compliant with ISO 27001 standards to advance information security management system (ISMS). IT-Grundschutz has evolved from ISO27001 because of its technical adaption while ISO standards are adjusted with business processes [11]. ISO 27005 security standard has a systematic approach to the development and maintenance of information security risk management process. The third version, the ISO/IEC 27005: 2018 provides a framework to manage cybersecurity risk effectively [12]. The security standard has three main phases in its risk management process: risk identification, risk estimation and risk evaluation [10].

The security standard that an organisation wants to maintain depends on the necessity and requirement of the organisation. The organisation that the payment gateway process will be

taken into consideration is licenced to be ISO27005 certified. Therefore when selecting the security risk management method the compatibility towards ISO27005 is considered.

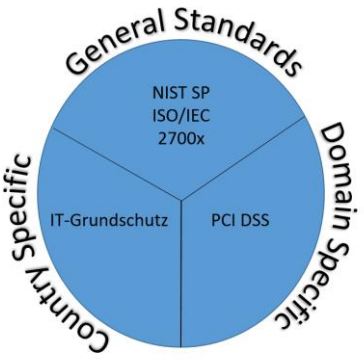


Figure 1: Security Risk Management Standards [11] [8] [7] [10]

2.2 Security Risk Management Methods

At present, there are numerous methods to conduct security risk management, and it is preposterous to find out the best as every method is unique and has pros and cons. A comparison of CORAS [13], MEHARI [5], OCTAVE [18] and ISSRM [5] methods are presented to identify what suits most to this particular thesis.

CORAS is one of the first security risk methods to have a model-driven risk analysis approach [13]. CORAS is aligned with ISO 31000 and has a language and a method which contains a practical and systematic guide. This method mainly consists of 8 steps, "*Initial preparations for the analysis, customer presentation of the target, refining the target description using asset diagrams, approval of the target description, risk identification using threat diagrams, risk evaluation using risk diagrams and risk treatment using treatment diagrams"* as indicated in [14]. It has a graphical language for modelling risks and threats. The approach is focused towards the protection of current assets [15] but direct, indirect and human assets will be considered as well during the target identification [16].

Method for Harmonized Analysis of Risk (MEHARI) is a risk management and risk assessment method which was developed more than two decades ago. MEHARI is a flexible method when defining the context establishments as it could be either apply to the entire organisation or narrow down to a business activity. Organisations can use MEHARI for auditing if the particular context is compliant with the ISMS process and also the design itself supports ISO/IEC 27005. Services, information data and compliance to regulations are types of assets considered in asset classification of the risk identification phase apart from stake analysis [5] [17].

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a self-directed risk-based strategic assessment intending to capture the current state of security practice in the organisation. The method is driven by operational risks and security practices aspects. It checks on strategic issues, focus on security practices and evaluate the organisation. Three phase approach of OCTAVE identifies what is important to the organisation with current mitigation techniques, infrastructure level examination to identify vulnerabilities and identify risks to the critical assets. Small/medium organisations and large organisations can use OCTAVE as it has two variants named OCTAVE -S and OCTAVE-Allegro which is compatible with large to small scale organisation [18]. OCTAVE method takes

consideration of employee participation during the risk management process. This approach uses critical assets to identify and prioritise areas for improvement. However, OCTAVE has organisational and technical differences which do not streamline with ISO27005 standards such as the dependency on workshops, people and the phases in the risk management process as per [19]. Additionally it does not reflect the relationships of different risks [20].

Information system security risk management (ISSRM) consists of a domain model which has been developed by combining security risk management standards, security risk management and a survey of security-related standards [5]. ISSRM is aligned with ISO 2700k standards as well as it considers system and business assets when conducting security risk management. ISSRM method is flexible as it does not have a dedicated tool or a modelling language in-built.

Comparing the risk management methods as shown in Table 1 illustrates what method is most suitable to compare security risks in in-house and cloud infrastructure.

Table 1: Comparison of Risk Management Methods

Name	**Support ISO/IEC 27005?**	**Threat Modelling Included?**	**Consider Infrastructure Components?**	**Tool Included?**	**Modelling Language independent?**
CORAS	NO	YES	YES	YES	NO
MEHARI	YES	NO	YES	YES	NO
OCTAVE	NO	YES	YES	YES	NO
ISSRM	YES	YES	YES	NO	YES

ISO 27005 does not have a particular method for risk management and the organisations are free to choose their own method which supports ISO 27005 in order to be compliant with the standard. CORAS and OCTAVE approaches have similarities, but both do not support ISO 27005 standards. One of the main facts to consider in choosing the RM approach is whether it considers business assets and supporting assets. OCTAVE consider both organisational and technical assets, but the main focus is driven towards critical assets. Therefore both approaches are eliminated as a suitable RM method. MEHARI is aligned with ISO standards, but it has an excel-based tool. Since the thesis is about finding the security risk gap of different infrastructures, a visualised diagram and the flexibility of choosing a modelling language is considered as a benefit. Therefore, ISSRM is chosen as the preferred RM method to conduct the risk analysis.

2.3 ISSRM and Domain Model

Asset identification is the first step to be followed in majority of risk analysis methods. However asset identification can have limitations based on the definition of RM method. ISO 27005 define asset as anything that has a value to the organisation therefore supporting assets are considered. Asset identification and classification is important to develop a secure system and mitigate security risks. As per figure 2, the first step of ISSRM process is to identify the context and assets. Afterwards, the security objective of business asset needs to be identified based on confidentiality, integrity, availability (CIA) triad. Risk analysis and assessment are done to identify what could harm assets and threaten security objectives. First three steps will be repeated until a satisfactory assignment is made before risk treatment

as it is decisive to identify the risks thoroughly in order to treat security risks. Figure 2 shows how ISSRM aligns with ISO27005 framework proving the suitability to conduct the RA for this research work. According to the ISO 27005 completing risk identification and estimation is considered as risk analysis and evaluating the risks makes the risk assessment complete. *Security objective determination* can be seen in ISSRM as a separate step additionally to the steps that are presented in ISO 27005 framework.

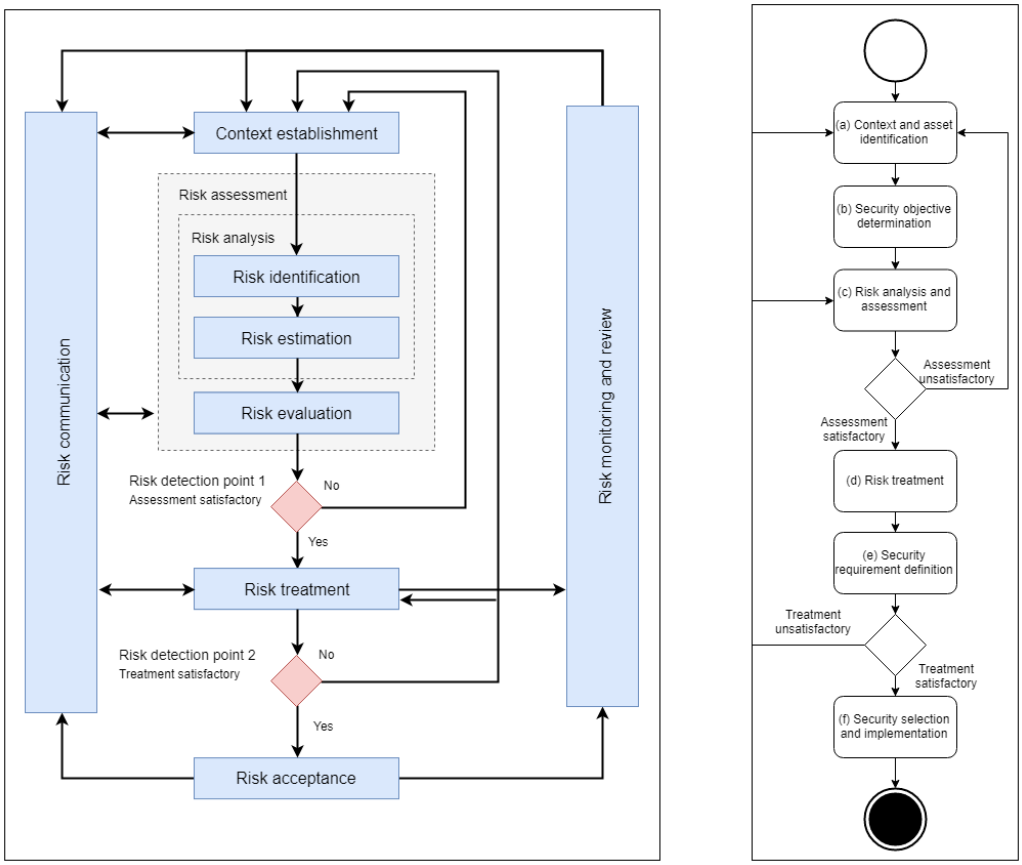


Figure 2: ISO27005 Framework [21] in left and ISSRM [5] in the right side

ISSRM has a domain model which has three concepts related to assets, risks and risk treatment as shown in figure 3 [5]. The following paragraphs which explain ISSRM concepts are based on [5].

In *Asset related concept*, an asset is considered as anything useful to the organisation in achieving objectives. Assets are divided as business and information system assets in ISSRM. Security objectives will be defined according to the *confidentiality*, *integrity* and *availability* of the business asset using value metrics while information assets are supporting asset to the business. If any information, process, capability or skill is required to the business, it can be categorised as a business asset. Infrastructure, software along with people engaged in the system is considered as an IS asset.

Risk-related concepts illustrate how one or more assets in an organisation could have an adverse *consequence of the risk* due to a combination of threats executed by a threat agent on one or more vulnerabilities in an information system. A potential negative consequence can affect both business assets and information assets directly or indirectly as data leakage

by a threat agent could have an impact on the confidentiality of customer information on a system. Risk level metric is used to assess the risk, and it depends on impact level and potentiality of the event.

The third concept of ISSRM domain model, "*Risk treatment related"* describes about treating the identified security risks. The decision can either be a *risk avoidance, risk reduction, risk transfer* or *risk retention* and this decision will be taken based on security requirements of an organisation.

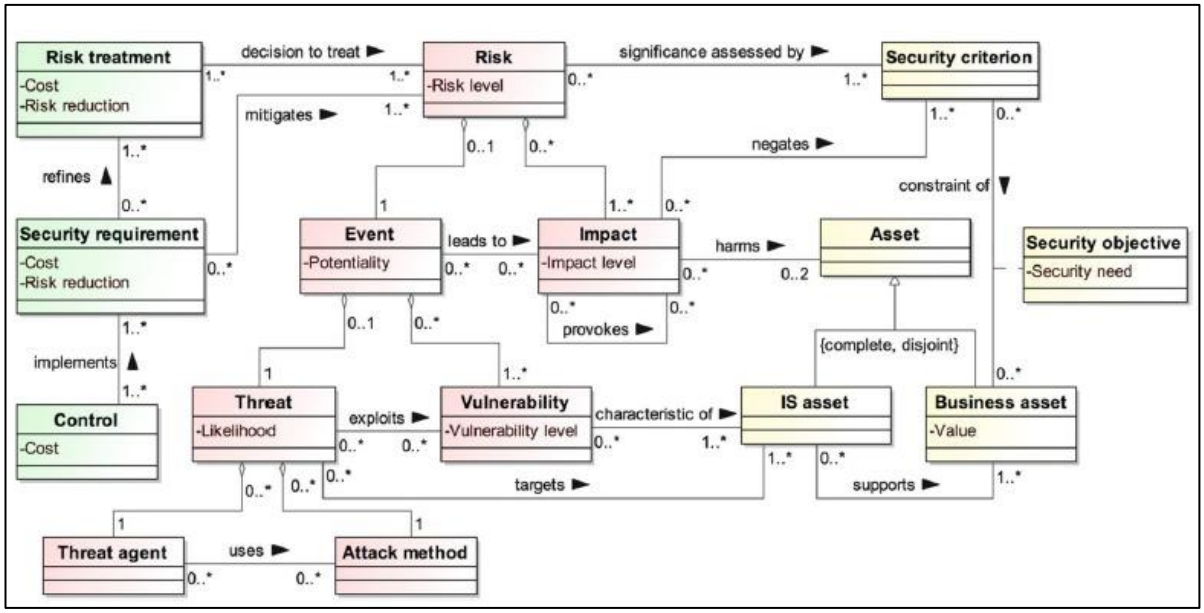


Figure 3: ISSRM Domain Model [5]

2.4 Modelling Languages

Modelling a system helps organisations to self-evaluate the requirements and completeness of the complex system while having a clear understanding about problems that was obscure during the initial stages. Furthermore, it supports to contrast the requirements and visualize the relationships of particular entities in various layers such as business, information technology layer [5].

Business Process Model and Notation (BPMN), is a modelling language for business processes which has a set of rules defined for linking objects with different meanings. BPMN itself is not built for security risk modelling. However, research [22] shows that BPMN can be compatible with ISSRM domain model to identify the context and assets in security risk management. This thesis is about comparing the security risk changes that can occur based on a migration. The business process diagram based on BPMN will only have a limited number of IS asset as the objective of BPMN is to model the business flow. Therefore a visualisation of business process mapped with underlying infrastructure is essential to identify the IS assets and the relationship with business processes to conduct the risk analysis.

The Enterprise architecture (EA), a concept which demonstrates the IT infrastructure and its alignment to business [23]. TOGAF is an EA framework for developing enterprise architectures [14]. In paper [24], authors have described the conceptual alignment of TOGAF and

ISSRM Domain model. However, TOGAF is an independent framework, which is not appended to any enterprise architecture modelling language [14]. But ArchiMate is an EA modelling language which can visualise different domains, and it is well aligned with the TOGAF framework [15]. As shown in figure 4, ArchiMate 2.1 has a three-layer representation which consists of business layer, application layer and technology layer. The three layer view of ArchiMate 2.1 is used to show the mapping of business to IT layer through the application layer.

Figure 4 presents three aspects that can be modelled with ArchiMate. Active structure presents the components of the layer and behaviours aspect present the services that each layer offers. The objects such as business objects, technology artifacts and data objects in application are represented using the active structure. The capability of modelling business and technology of ArchiMate is used in the study to identify the architectural differences between in-house and cloud and to conduct the threat modelling to the IS assets.

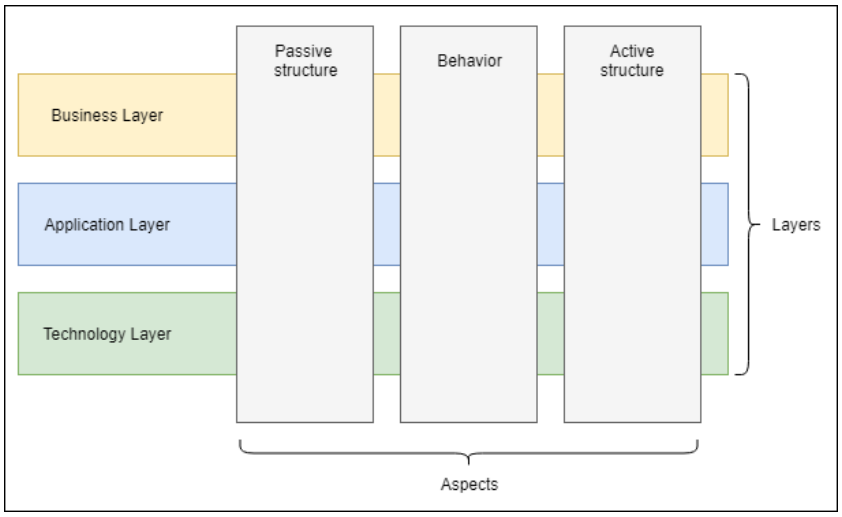


Figure 4: ArchiMate Core Framework, adapted from [25]

There is a limited number of modelling languages available for infrastructural modelling such as CySeMol [26], UML Class diagrams and SecuriLang. The software systems available for CySeMol is outdated, and SecuriLang is built by improving CySeMol language [27]. SecuriCAD tool developed by Foreseeti [23] uses SecuriLang infrastructure modelling language and can be used to illustrate the low-level view of infrastructure components and the relationships of the entities [28]. However SecuriCAD tool has development bugs and some were reported during the research. In conclusion, during the research, only BPMN and ArchiMate modelling is used.

2.5 Threat Modelling

Information systems interact with other systems and can be operated in multiple infrastructures by different user groups. All the IS assets does not hold same level of importance as system requirements and goals can be different. Treating all the system assets equally cannot be considered as a good approach when it comes to security risk management. Processes

that holds critical information needs to have more attention. Thus, a company should prioritise assets based on the company requirements. Security engineering focus on reducing unauthorized harm, which is intended against an asset. Predominantly, the attention towards security and risks have not been taken into consideration during early stages of system development [22].

As per [5] risk, is defined as a "*Combination of a threat with one or more vulnerabilities leading to a negative impact on two or more assets by harming them*". Therefore identifying the possible threats to assets are a necessity. A survey [29] was conducted regarding different threat modelling approaches where some are dedicated to RM methods while some are not attached to a specific RM method. Attack trees, CORAS, STRIDE are some of the threat modelling methods that have been examined in the survey.

STRIDE threat modelling methodology was invented by L. Kohnfelder and P. Garg [30] and has been in the industry since 1999. A previous study [31] about *Risk management in E-commerce system* has applied STRIDE as a threat modeller to identify threats while following the ISSRM and it has shown the compatibility of using STRIDE along with ISSRM.

Therefore, threat identification in this study will be based on STRIDE. STRIDE can be used to focus on processors, data and entities. STRIDE taxonomy gives an approach to identify threats in the systems by categorizing it into six threat types. Table 2 shows the STRIDE categories and their descriptions.

Table 2: STRIDE Threat Categories [30]

Threat category	**Security property violation**	**Description**
Spoofing	Authentication	Impersonating something or someone that is not intended to be
Tampering	Integrity	Modifying something in infrastructure or the process
Repudiation	Non-repudiation	Claiming that someone or something is not responsible for an action that has happened.
Information disclosure	Confidentiality	Exposing information to parties not authorized
Denial of service	Availability	Make services unavailable by deny, degrade or utilizing the resources intending to make the service unavailable
Elevation of privilege	Authorization	Doing a particular thing that a party is not intended to do

2.6 Related Work

Related work helps to identify the research gap and to continue with the finding that was presented earlier. Thus, this section will focus on enterprise architecture, threat modelling in infrastructures and risk management related work which focuses on business processes.

The research [32] proposes a novel approach for risk assessment through the use of EA. The objective of the work is to bridge the gap between the technical and business views of systematic security risk assessment. Through the proposed approach, the author has tried

to reduce the complexity of the business process in supporting assets by illustrating an abstraction that shows the interdependencies of each layer. This study describes the alignment of EA from asset identification to risk treatment. However, the research work has not been implemented in a case study.

Cloud computing threat analysis is written in several papers including those that conduct quantitative and qualitative analysis. In paper [33], the authors present threat modelling for cloud infrastructure. The intention of the research is to provide potential threats and mitigation techniques for the cloud infrastructure because there has not been much research conducted on infrastructural threat modelling even though cloud computing is trending. The study focuses on several threat modelling and threat measuring techniques applied to a real world cloud infrastructure. Attack trees, attack graphs, and attack surface analysis, are the threat modelling methods used by the authors. This paper helps the cloud providers to identify and harden the security of the cloud. However, business layer modelling and the interdependencies of business and infrastructure is not presented in this study. In study [34] STRIDE based threat identification on cloud was conducted. Authors motivation towards writing this paper is to present threats and risks based on cloud. But author is not considering the impact on assets. Furthermore, this paper is based on generalized threats in the cloud environment.

Research work [35] " *Security Risk Management in the Aviation Turnaround Sector* ' is a research which used ISSRM to analyze the cross-organisational collaborations. Author has modelled the business layer and followed the ISSRM domain model, but visibility of infrastructure associated with the business layer cannot be seen in this work. The author has mentioned analyzing security threats in cloud-supported enterprise collaboration as a future work. The doctoral thesis [36] has provided a method for risk analysis of the virtualized systems. The author has illustrated how useful it is to do the risk assessment not only to the infrastructure but the process flow as well. One of the scientific novelty of the thesis is the introduction of a numeric procedure combining exploit scores and its probabilities. The in-depth analysis of the threats in virtualization systems in multiple perspectives had added value in the evaluation phase. Cloud computing is one of the main forms of virtualization and it is favourable to have a proven risk assessment methodology aligned with a thread modelling technique which is flexible to compare the cloud as well as the on-premises infrastructure for a client who needs to compare how risk could change in virtualized environments and in-house infrastructures. Detailed description of relationship representation of the components and tasks of different layers were not highlighted.

The author of the paper [37] has used ArchiMate for enterprise architecture modelling to manage security risks. The Author's goal was to present the alignment of EA to SRM. The author has only shown high-level mapping, but low-level modelling of each layer and the relationship between business assets and its relating information assets has not been the focusing point. Previous research work [14] describe the complexity of information security RM and the need for integrating EA modelling with ISSRM. The objective of the paper is to take the ISSRM domain model to be extended as a framework which consists of a method, language and a tool. TOGAF was used as the EA framework, and the alignment of ISSRM along with TOGAF is described clearly by highlighting the relationships of both concepts. The focus was on integrating the two models, and this was not applied to a real-world scenario. The authors have not presented the usability of EA and ISSRM for risk assessment. The integration of asset related concepts are used in this study. Research work [38] shows the modelling of security concepts and its corresponding relationships with Enterprise architecture. The compatibility of ArchiMate with EA frameworks have also been described.

The study does not present a risk management approach considered in the work even though the design models related to risks concepts are properly presented.

The cloud infrastructure, risk analysis and threat modelling related research has been conducted in the past.

But during the literature review, it revealed that EA based risk analysis approach to compare infrastructures were lacking. Therefore the study will focus on how EA based security risk analysis can be used to compare security risk changes between different infrastructures. Also this study is based on a real world implementation.

2.7 Summary

Chapter two presents the theoretical background of security risk management methodologies and standards. A comparison was made to identify the most suitable risk management methodology, and ISSRM was chosen due to its systematic approach and the categorisation of different concepts in the domain model. This thesis will illustrate how infrastructural change would affect the risk analysis process. Since ISSRM is modelling language independent, BPMN was chosen to model the business process. ArchiMate will be used for enterprise architecture modelling and the relationship between the layers will be presented via ArchiMate EA model. STRIDE threat modelling methodology is used for threat analysis of the traditional in-house infrastructure and the cloud infrastructure. Table 3 summarises the chosen approaches to perform a comparison of security risk in the in-house infrastructure and a cloud infrastructure.

Table 3: State of Art Abstract

Category	**Name of chosen method /language /type /diagram**
Risk management method	ISSRM
Type of assets	Business and IS assets
Types of infrastructures	In-house infrastructure and cloud infrastructure
Business process modelling language	BPMN
Business asset and infrastructure mapping framework	TOGAF
Business asset and infrastructure mapping language	ArchiMate using Archi software
Threat modelling method	STRIDE

3 Context of the Study

Chapter 3 focuses on providing answers to RQ 1. RQ 1 is supported by three sub-questions and the chapter describes the architectural differences between in-house infrastructure and cloud infrastructure.

RQ 1: **What are the architectural differences between in-house infrastructure and cloud infrastructure?**

RQ 1. 1: What is the in-house infrastructure of payment gateway system?

RQ 1. 2: What is the cloud infrastructure of payment gateway system?

RQ 1. 3: What can be used to model in-house and cloud infrastructure?

3.1 Payment Gateway System

Information and communication technology (ICT) has established its roots in diversified fields and e-commerce has been one of the instances. E-commerce has opened the gates for merchants and buyers by providing the opportunity to buy and sell without any geographical boundaries. When the number of e-commerce appliances increased, an application was built to process payments by acting as an intermediator for financial institutes and merchants. The security risk analysis of the research is based on this intermediator which is the payment gateway system. A system is a group of components interacts and interconnect for a common goal [5]. Table 4 presents examples of system components in payment gateway system.

Table 4: Payment Gateway System

System Components	Case Study Examples
Product/ Components	Database, PayGate UI, Payment processing system
Infrastructure	Web application servers, Load balancers, Firewalls, Network and Devices
Application	PayGate app and Fraud app
Information Technology Staff	Application support, DB support, Developer
Users - Internal	Webshop merchant
Users - External	Webshop customer
Environment	Northern Europe

The study is based on the payment gateway system PayGate. PayGate provides service to more than 21 EU countries and 110 merchants are using the multi-channel payment solution. Availability of payment gateway process is important for an uninterrupted service to the customers apart from protecting confidentiality and integrity of information and processes. Payment gateways are categorised based on the integration method it uses to connect with a merchant. Hosted and self-hosted are the integration methods of payment gateways [39].

3.1.1 Hosted Payment Gateway

Hosted payment gateway redirect a customer to the payment service providers system to enter payment details during the checkout process. Payment details are not captured by the webshop because of this redirection. Placing an iframe of the payment gateway inside the merchant store is alternation for redirection to a payment service provider (PSP) page during the checkout. Since the customer is providing credit card information directly to the payment gateway system, the e-commerce site does not require to be PCI compliant. Examples: PayPal, 2Checkput and Payza.

3.1.2 Self-hosted Payment Gateway

In self-hosted payment gateways, the webshop collects customer payment details during the checkout process. The API integration is used to send the captured payment detail request to the payment gateway by the webshop. Therefore the customer will not enter the payment details directly in payment gateway.

3.2 Technical Infrastructure

Technical infrastructure exist based on a combination of components such as software, network, hardware and people. The organisation of the PayGate is planning to move the payment gateway system into the cloud infrastructure. Therefore detail analysis of current infrastructure is conducted to find the changes to architecture before the cloud migration.

3.2.1 Infrastructure of In-house Payment Gateway

The case study of PayGate infrastructure is based on the same premises as the organisation. The infrastructure is non-virtualised and consists of routers, web application firewall, hardware security module, data stores and load balancer. Cardholder data environment has been separated from order management, fraud checking and merchant support systems. The infrastructure that will be considered in this thesis consists of physical and logical separations, hosted in the premises of the business. Employees of the payment gateway organisation are conducting the maintenance and management of servers. The current infrastructure is holding credit card information of more than hundred merchant services and the payment gateway has been in the market for around five years.

Infrastructure details of PayGate system was gathered by interviewing domain experts. Furthermore, network maps, hardware details web application firewall (WAF) and past vulnerability reports were analysed. The in-house infrastructure web application firewall is a software-based firewall configured with Apache ModSecurity. Hardware security module in the diagram is a physical device used for cryptoprocessing [40]. This module is connected to the datastore which has payment details stored. In the payment gateway system, internal applications are developed by PayGate employees and third part application refer to applications such as Fraud app which is used in the environment to check the customer's legitimacy. The fraud rules are managed by PayGate.There are two types of firewalls in the environment and one category is software based and one category is hardware based. Since this is a PCI environment, every quarter a vulnerability scan is conducted. However, there isn't an automated mechanism to authorize access of the people to the Server room and this access is controlled by a security guard. Video surveillance is available as part of PCI requirement and it is yet a intrusion detection system.

3.2.2 Cloud Infrastructure

The adoption and use of cloud computing technology has risen greatly since the late 2000s, with much encouragement from companies such as Google, Amazon, Microsoft, IBM, and Rack space as seen in their cloud solutions [41]. Businesses migrate to cloud datacentres do not need to acquire and maintain large IT technologies on-site but instead, access these IT resources, from a remote location which is often managed by cloud service provider. Cloud is categorised to three main models such as infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS).

In IaaS, the service provider will give access to computing resources in the virtual environment allowing the customer to access computing resources from a hardware resource pool. These resources can be distributed to provide reliability and to avoid single point of failures. The customer is responsible for the installation of required software, applications and internal firewall separations [42]. Most of the cloud solutions are based on type 1 hypervisors and virtual machines are built on these hypervisors. Resources such as CPU, memory and network is shared among different customers. Policies and procedures towards maintaining hardware is important and clear segregation of responsibilities will avoid threats to systems. Example: Threat due to an unpatched hypervisor could make all the virtual machines in the host to pose a security risk.

In PaaS, customers get the opportunity to develop, deploy and manage the applications by themselves on a pre-installed platform or with necessary tools. Since the platform is dependent on the service-oriented architecture, the issues related to this architecture such as DOS, XML attacks, injection will be automatically inherited.

In SaaS, the customer will get inbuilt applications hosted in infrastructure of service provider. This service is available via the internet and hosted on the platform. The main security countermeasures that service providers must be responsible is that they should keep the applications patched accordingly and web configurations should be correctly configured. One key difference between IaaS, PaaS and SaaS is the level of control that the customer has in the cloud stack as opposed to the level of control for cloud provider.

Resource sharing and boundaries of deployment will be based on the cloud deployment model. Public cloud is a cost-effective solution compared to private, community and hybrid deployment models. Reports shows enterprise migration to cloud will grow within next two years [3]. Therefore, public deployment model is considered in this study.

According to NIST SP 800-145 [58], "*The cloud customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e. g. , host firewalls)*". Figure 6 shows what types of systems needs to be taken care by the cloud service provider in terms of security. Furthermore, dynamic nature of the IaaS environment (e. g. , with creating, removing and migrating VMs), present more challenges in the defence against cyber-attacks to the system.

Cloud concept and its use in the industry is not new, but responsibilities needs to be clearly identified by the cloud service provider and customer, to identify who needs to protect a IS system from a threat. However, the responsibilities can be dependent on the deployment model or architectural model [43]. Figure 5 shows the abstract of the shared responsibilities of the customer and cloud provider.

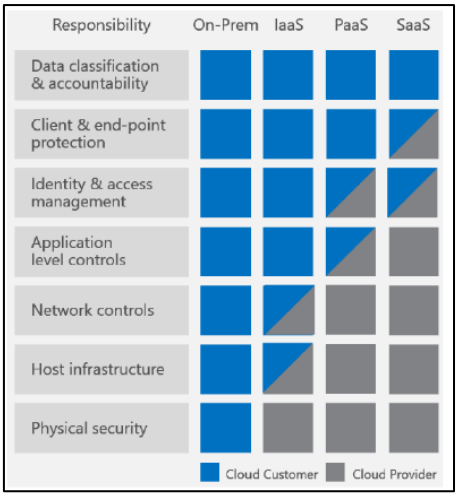


Figure 5: Shared Responsibilities of Cloud Customer and Cloud Provider [44]

3.3 Enterprise Architecture of the Payment Gateway System

Architecture of organisations are complex due to the distribute nature and integration of modern technologies. Architecture is basically a structure with a clear perception which presents the interdependencies and interrelationships of business processes and information systems [45]. Systematic modelling capability of EA helps to capture dynamic changes of infrastructure and dependencies. Therefore, pre-migration and post-migration infrastructure of the payment gateway system is modelled using EA modelling language named ArchiMate 2. 1.

As shown in figure 6, ArchiMate EA model contains three layers: Business Layer, Application Layer and Technology Layer. Business layer contains business services and business processes. Application is the intermediatory layer because it supports the businessess processes and services by providing software services and these services are hosted in the technology layer. Technology layer has the hardware, networking and facility components and it offers services needed to run applicaitons. In-house EA and cloud EA is modelled to find the changes of architectural components and the links between business process and the infrastructure. An assumption was made that the tasks of business process remained same while the infrastructure will be changed. In both, ISSRM and ISO 27005 standard “people” are considered as an IS asset and it can be divided as internal parties and external parties.

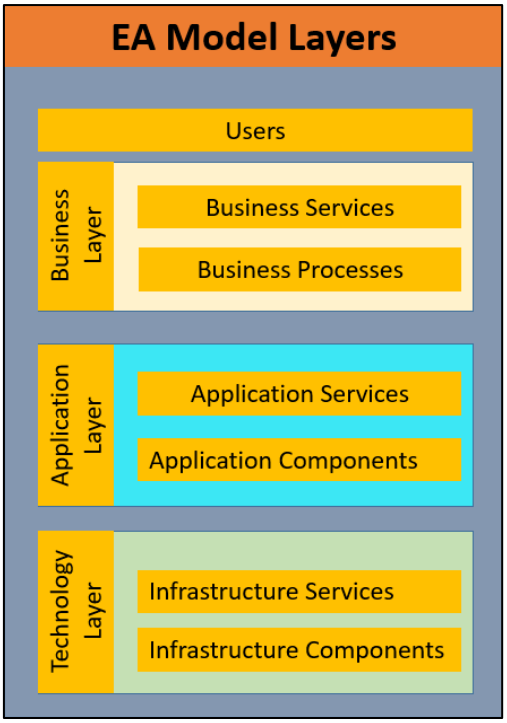


Figure 6: EA Model Layers [38]

3.3.1 In-house Enterprise Architecture of PayGate System

Analysis of the cardholder data environment in PayGate helped to identify the main processes and its sub processes. According the requirements, and information gathered, three layers were modelled. Business layer gives the overview from business perspective and technology layer of figure 7 presents the infrastructural components of the in-house payment gateway system. The technology layer first level abstraction as seen in figure 7, was modelled using the network map of the environment. Interdependencies of business layer to technology layer was modelled after a thorough analysis. Given below provides an example of how EA modelling will ease to find the underlying technology of a business process and hence to find out the corresponding IS assets.

Example: Customer (user group) receive "Accept order payments" (business service) from Payment transaction process (a process in business layer) and Payment gateway application and Order management applications are used to provide Process credit card data, PSP connection and "Process order information" application services to the Payment transaction process. These applications are directly linked with technology layer services such as host payment gateway, generate logs, databases service and application hosting services. The infrastructure that provides those services are support zone, Application server farm and Webshop. Figure 7 diagrams illustrates the high level abstraction of in-house EA of the payment gateway system.

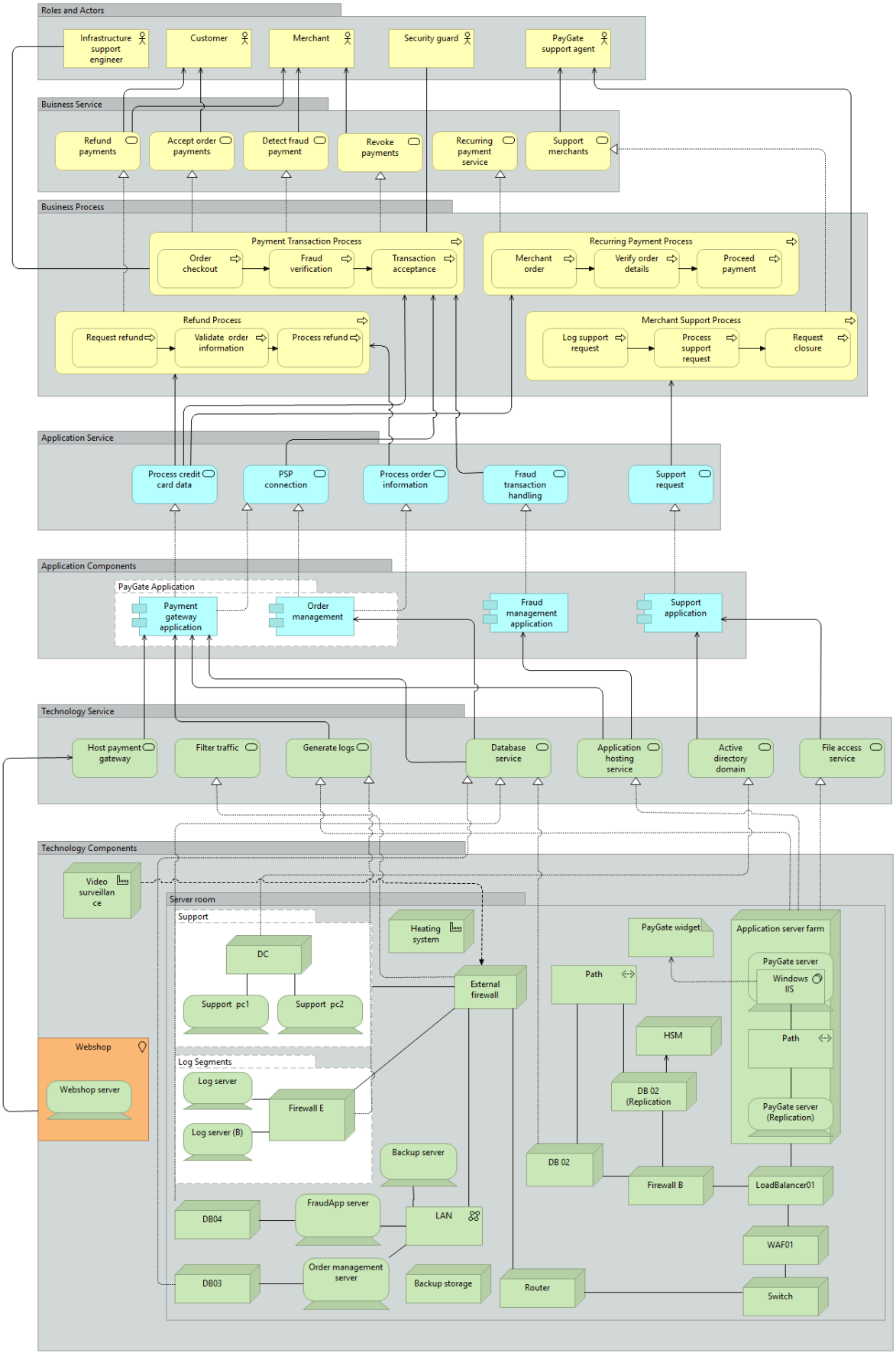


Figure 7: ArchiMate Model of In-house Infrastructure

In figure 7, EA model of in-house presents five actors. The business layer consist of business services and business processes. There are four business processes in payment gateway system represented in the business layer. Those are, payment transaction process, recurring process, refund process and merchant support process. These four business processes does not access the same technology component or applications. The abstract present how these processes are connected to technology layer. There are four applications hosted in the application layer. Order management has its own application but mainly connected with the PayGate application. Fraud app and merchant support applications are not developed by PayGate company, but has full control over the application configuration. Hardware, network and facilities are presented, but does not reflect all the components or relationships as this is a high level diagram. Infrastructure support engineer and security guard is only mapped with paymenet transaction process. These two actors needs to be linked with other processes as well. However the links were not presented to reduce over complexity of the diagram.Backup storage is interntanally not connected as it is stored seperately.

3.3.2 Cloud Enterprise Architecture of PayGate System

Cloud technology layer was modelled using the information gathered from popular cloud providers such as OpenVAS, Amazon and Rack space. The cloud model presented in this work is generalized. The environment of the cloud data centre is not dedicated and therefore cloud co-tenants might be residing in the same hypervisor even though there is a network separation. Storage services and shared resource pool is accessed by all the co-tenants networked to the storage. Cloud maintenance users are considered out of scope due to the highly distributed nature of vendor supporting involved in cloud services. Cloud has advanced functionalities and the technology in use are different. Example: Cloud data network. Major architectural difference between cloud and in-house infrastructure are, cloud has components related to virtualization. Switches, networks in the cloud are mostly logical separations. Cloud has shared resource pooling in order to facilitate the growing need of resources. Therefore storage access cannot be segregated from other con-tenants in public cloud. In the cloud architecture also the same business processes can be identified due to the assumption made in the scope of study.

Among the business processes modelled in both infrastructures, payment transaction processing will be taken into consideration. The expansion of payment transaction process will be discussed in chapter 4 to elicit the business assets. Figure 8 presents the abstraction of the cloud data centre and the integration with PayGate business processes.

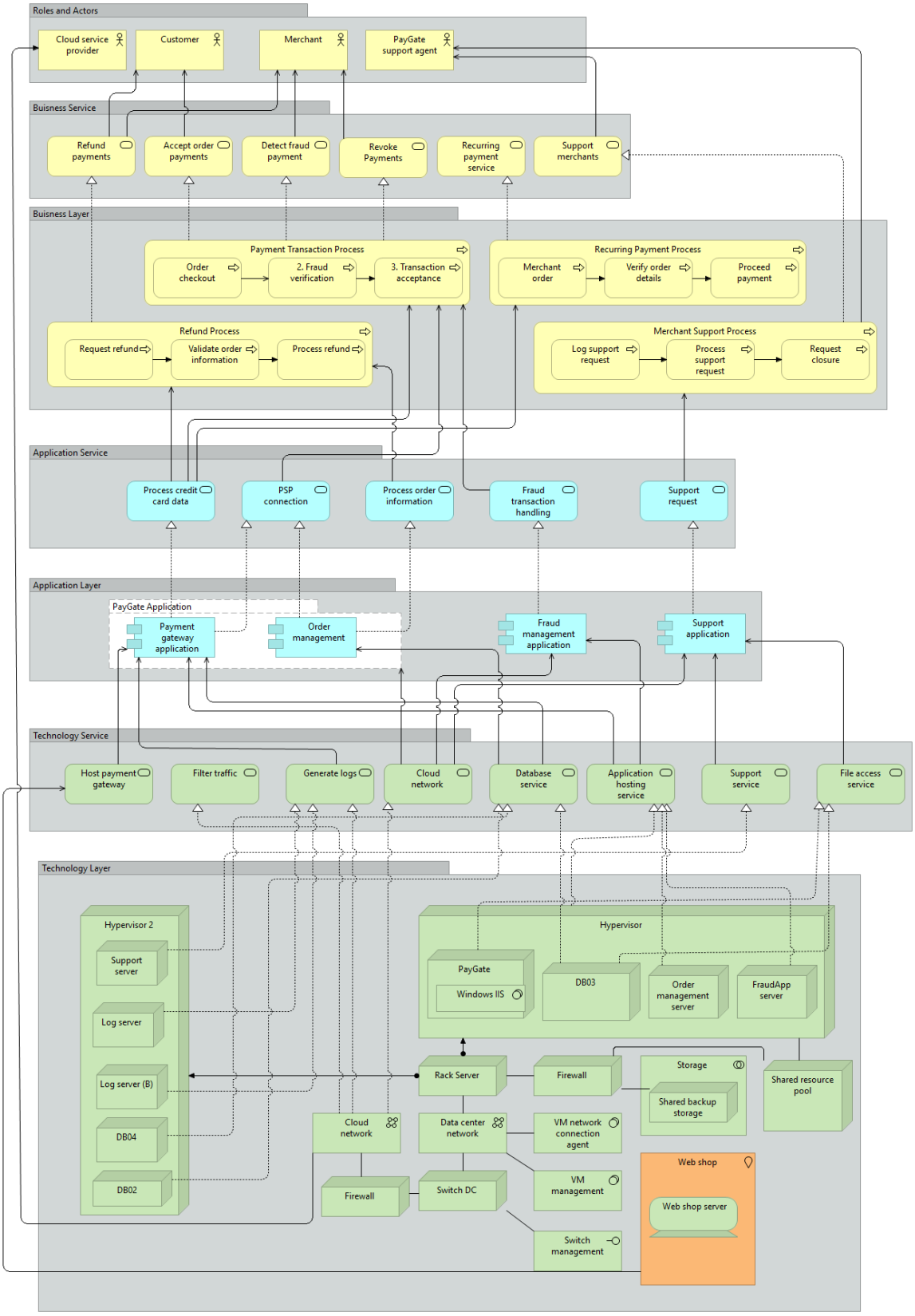


Figure 8: ArchiMate Model of Cloud Infrastructure

3.4 Summary

The chosen study will present a hosted payment gateway process where the webshop will not need to store credit card information and the payment gateway will handle the customer credit card information. The chapter is about finding architectural differences of in-house and cloud infrastructure. Firstly a thorough analysis of the in-house data centre was conducted by interviewing people and analysing the documents related to the environment. Cloud model was created based on research models that are publicly available. EA modelling is used in this chapter to visualize the differences from an abstract level to get an understanding of the differences before and after a migration to cloud infrastructure.

The in-house is based on a non-virtualised environment and cloud infrastructure in EA is based on a virtualised environment. In cloud environment cloud service provider will have access to the environment while in-house security guard will not be presented in the cloud. The major technology level component change that can be seen is the virtualization based changes such as shared resource pool and cloud specific network configurations.

4 Asset Identification of Payment Gateway System

Chapter 4 focuses on providing answers to RQ 2. RQ 2 is supported by three sub questions and the chapter helps to elicit business assets and IS assets from in-house and cloud infrastructure.

RQ 2: What are the business assets and supporting information system assets?

RQ 2. 1: What to use to identify and elicit assets in in-house and cloud infrastructure?

RQ 2. 2: What are assets in-house datacenter and cloud infrastructure?

RQ 2. 3: What are the security need of business assets?

Asset identification of a given context needs proper analysis as it will present the organisational assets to be protected and helps to identify the security objective of each business assets. Assets that will be considered in risk management is dependable on the method chosen as asset definition and asset capturing differs from one RM method to another. Poor identification of assets and insufficient attention towards generalized risks can lead to potential harm. To have better visibility of the business assets worth protecting, a visualization of the business process is presented in this chapter. The connectivity of information system with business assets is represented via ArchiMate through the application layer in Chapter 03 as the first abstract level model. Figure 9 presents how assets are elicited using modelling languages. In chapter 3, ArchiMate 1st level diagram is presented. In chapter 4, an expansion of Payment transaction process is made using BPMN. Order details in the figure 9 is to represent that only one asset will be chosen and modelled with associated system assets.

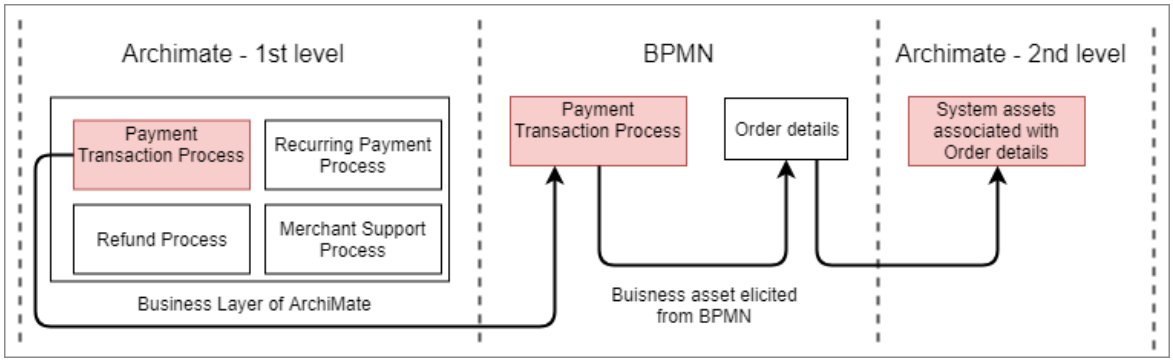


Figure 9: Model based asset identificaiton

4.1 Business Processes of Payment Gateway System

Payment gateway process is the bridge between customer and financial institute which handle transaction details on behalf of the merchant. Merchant will send a request to the payment gateway company asking for the service to be integrated. The case study is based on a hosted payment gateway which uses Widget API.

Payment gateway system is a combination of multiple processes and failing to meet security requirements in one process can lead to critical harm in other processes due to the interdependencies. Figure 10 shows the value chain of payment transaction process derived from the enterprise architecture business layer. Appendix 1 contains the BPMN diagram of Payment Transaction process.

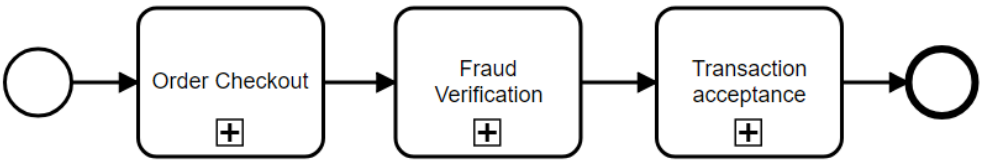


Figure 10: Value Chain of Payment Transaction Process

Payment transaction process has three sub processes:

1. Order Checkout
2. Fraud Verification
3. Transaction acceptance

Order checkout process starts when the customer proceeds to checkout. The webshop will request for available payment methods for a chosen shop from PayGate and it will send the response with a security token which is used to uniquely identify the transaction. Payment gateway iframe will be loaded afterwards this study is based on a hosted payment gateway. Customer will enter the payment details and this details will be encrypted using AES 256 and sent to the PayGate. The webshop will not see the credit card details as customer payment details will sent to PayGate without transferring it to webshop. Payment details has customer credit card number, CVV and expiry details. If the payment details validation passes, webshop will send Order details to PayGate. Order details contains customer name, customer DOB, customer email address, shipping address, customer address, order ID, order item, quantity and price. Figure 11 presents the Order checkout process.

When PayGate receive Order details from the webshop, it sends details to be checked against a fraud database. The check is conducted by comparing email addresses, shipping addresses and past transaction records. If the customer is identified as fraudulent, webshop will be informed. Figure 12 presents the Fraud Verification process.

PayGate will connect to the PSP layer if the request comes till *process the payment* task as seen in figure 13 PSP layer will send a response back to the PayGate about the status of the transaction based on the response it received from the bank. If the payment has been declined by the bank a notification will be sent to the customer and the order cancellation happens. If the payment is successful, the webshop delivers the message to the customer and notify the shipping process which is out of scope in this study. Figure 13 presents the Transaction acceptance process.

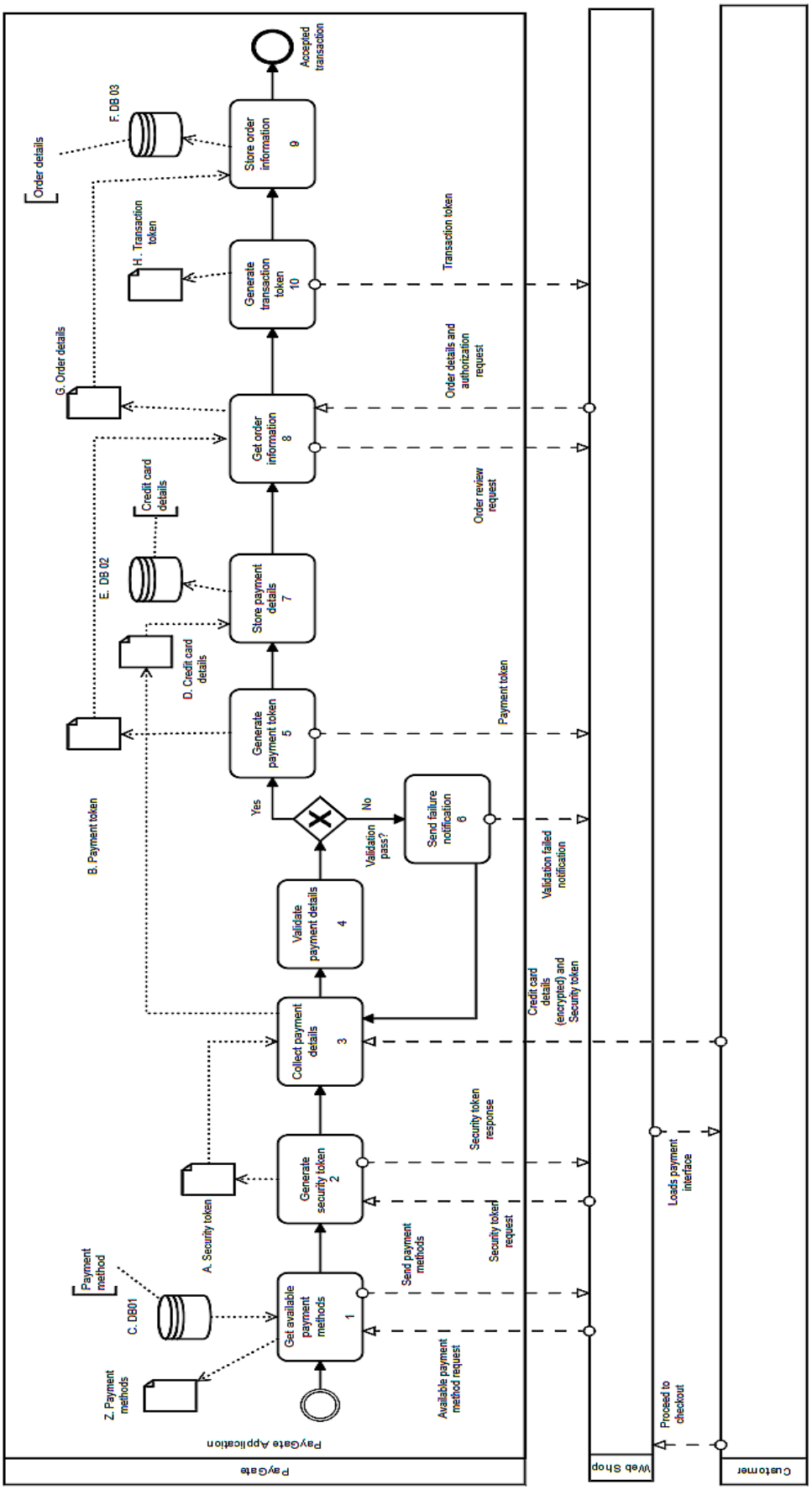


Figure 11: Order Checkout Process

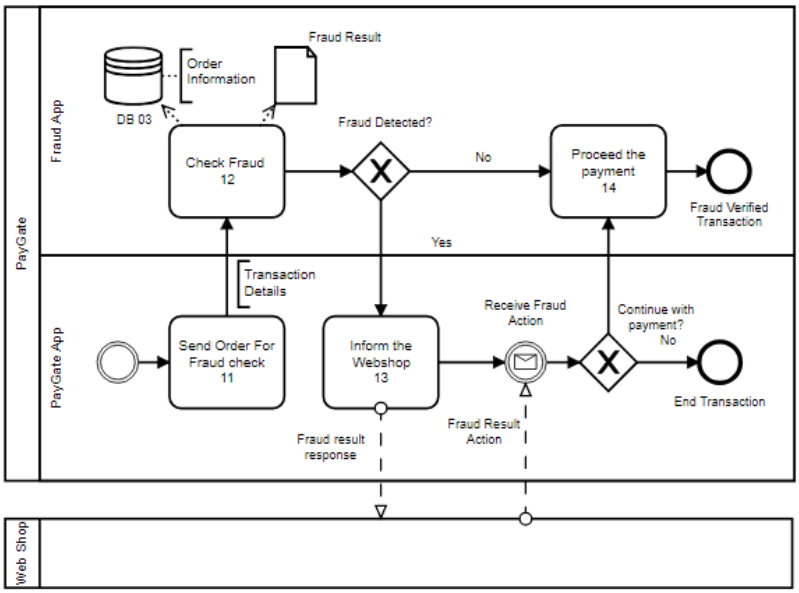


Figure 12: Fraud Verification Process

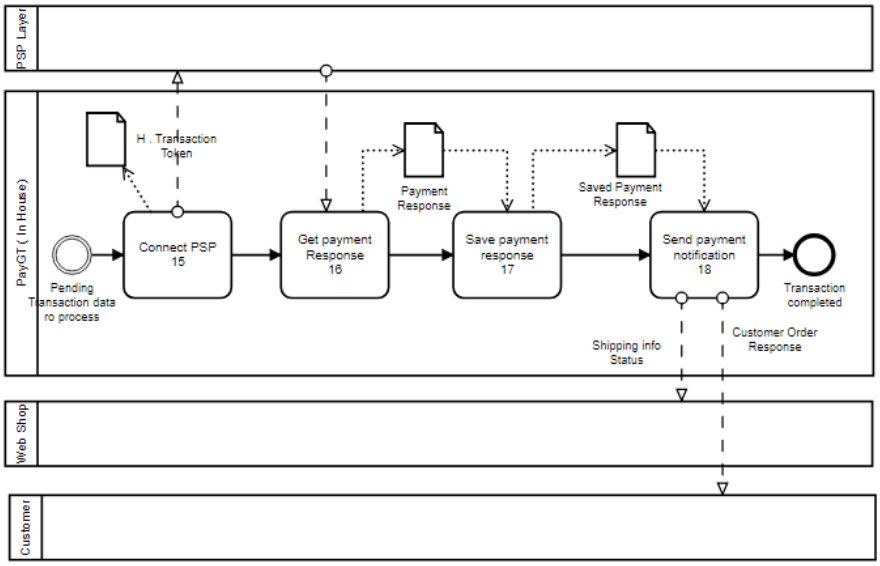


Figure 13: Transaction Acceptance Process

4.2 Security Objectives of Business Assets

According to ISSRM, determining the security objectives of the context and asset identified is listed as the second step of the ISSRM process. Security objective can be generalized as the need of defining the level of assurance or protection of the information systems and the information from any kind of action which would lead to destruction, unapproved access, disclosing information, modifying, using systems and data or interrupt the service.

Security Objectives are mainly categorised as *Confidentiality*, *Integrity* and *Availability*, however the level of each property needs to be maintained is decided by the criticality of the asset and the context of the business [46].

Confidentiality: This refers to that restriction of disclosing information to parties that are unauthorized to access in order to protect the privacy of people and proprietary information.

- Example: A server in a PCI environment needs to have adequate protection of the data because it stores/transmit credit card information. If an unauthorized party can view the credit card information, then it violated confidentiality of the information.

Integrity: This is the property of ensuring that the assets are not altered or deleted by unauthorized party and it maintains the accuracy.

- Example: A malicious actor changes the recurring information consent of a customer and a customer will not be charged the appropriate amount of money for the service subscription.

Availability: Property which assure that authorized assets can be accessed without any interruption in required time.

- Example: An attacker utilize the resources of the payment gateway and make the payment widget unavailable to the users who wants to purchase an item from the webshop.

A security risk can harm one or more security objectives of a business. There are supporting security objectives to the CIA properties that are related to the users who use information or interacts with different business assets. *Authentication* means the verification of who you are by using what you know, what you are or what you have [47]. *Authorization* determines what permission level a particular person intended to have once authorized. Non-repudiation means the assurance given on a particular activity cannot be rejected or denied or be accountable for the actions.

Defining the level of security objectives on different environment can be contrast from one another. Understanding the security objectives and evaluating the controls for protections can be somewhat difficult in cloud infrastructure, because the responsible party of security cannot be limited to service provider or either buyer/customer. It can be defined as a handshake where both parties equally contribute and should be cautious about the security as a breach from either side can lead to major disasters and violate the security properties. Table 5 shows the Business assets derived from the BPMN diagram with the security objective of each asset.

Table 5: Businessness Assets and Security Objectives

BPMN Reference	Business Asset	Primary Security Objectives		
		C	I	A
A	Security Token	x	x	
B	Payment Token	x	x	x
D	Credit Card Information	x	x	x
G	Order details	x	x	x
H	Transaction Token	x	x	x
Z	Payment Methods		x	x
Y	Fraud Results		x	x

4.3 System Assets of Payment Gateway System

After eliciting the business assets and determining security objectives, one asset was chosen to further model and expand the technology layer. This expansion was modelled using ArchiMate. Order details were chosen among the business assets elicited. Figure 14 and Figure 15 contains an expansion of both infrastructures.

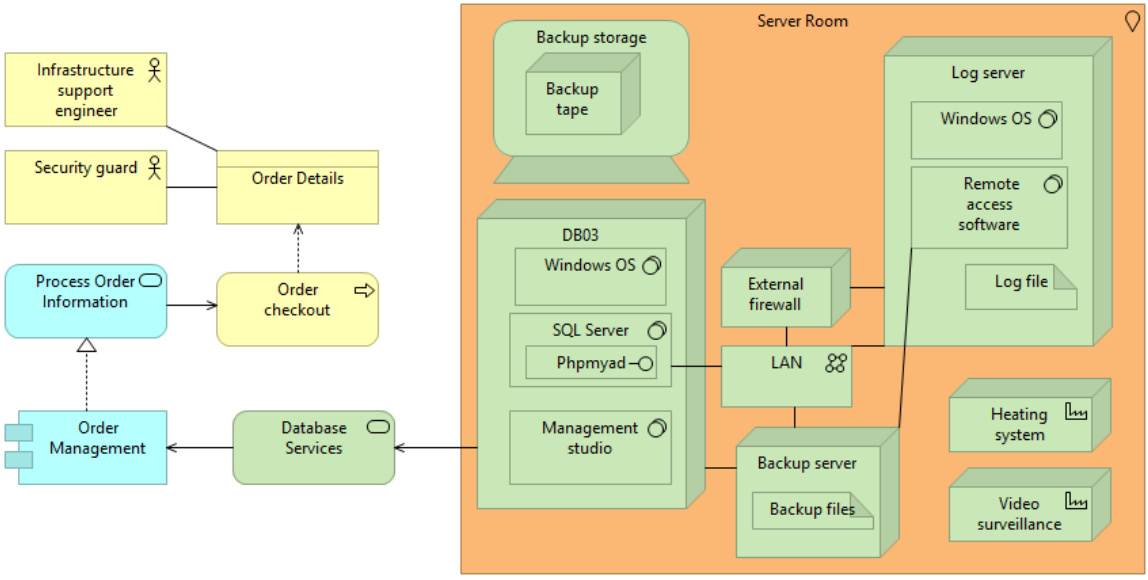


Figure 14: Order Details Mapped to Architecture Components of In-house

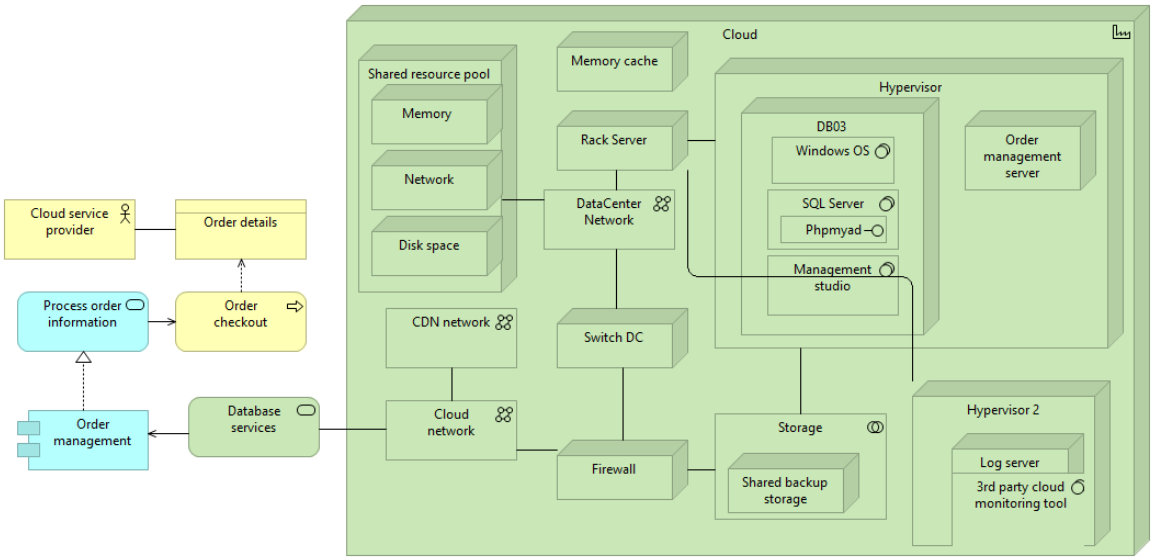


Figure 15: Order Details Mapped to Architecture Components of Cloud

Figure 14 and figure 15 was modelled based on the first level archimate diagram presented in chapter 3. Order details were derived from the payment transaction process and the technology layer was expanded based on the mapping on buisness to appplication and technology layer. Table 6 shows the system asset components of in-house architecture and cloud architecture that will be used on the risk analysis. This table is not a comparison of IS assets that could exist in in-house and cloud infrastrcure. Some of the assets presented

in in-house can also be presented in cloud. However the reason why it has been shown in the table is becasue of the premises it is based on.

Table 6: System Assets of Infrastructures

System Assets	
Components of In-house Architecture	Components of Cloud Architecture
External firewall	Cloud service provider
Security guard	Shared resource pool
Video surveillance	CDN network
Backup tapes	3rd party monitoring tool
Infrastructure support engineer	Shared backup storage
DB03 (Server name)	DB03
Heating system	Log server
Log server	

4.4 Summary

The objective of the chapter is to expand a selected business process from ArchiMate diagram in Chapter 03. Payment transaction process was chosen to be modelled with BPMN. In this chapter an assumption is made that the process flow of the business flow will remain same even the infrastructure changes. Security objectives were identified for the business assets derived from BPMN diagram. To find out the IS assets of in-house and cloud infrastructure to the specific business asset, Archimate second level modelling is used.

5 Risk Analysis of Payment Gateway System

Chapter 5 is focuses on providing answers to RQ3. RQ3 is supported by three sub questions and the chapter consists of security risk analysis and providing security risk scenarios of in-house and cloud infrastructure.

RQ 3: What security risks change when a payment gateway system migrates from in-house to cloud infrastructures?

RQ 3. 1: What are security threats in in-house infrastructure and cloud infrastructure?

RQ 3. 2: What are security risks in in-house infrastructure and cloud infrastructure?

RQ 3. 3: What are the differences and similarities of security risks after migration?

5.1 Global Payment-based Risk Overview

According to 2017 reports by Statista shows that 1. 66 billion of people in the world are online buyers and it is expected to grow another half a billion by 2021. Among the digital buyers 42% prefer to pay with credit cards [48]. These payments are handled by payment gateway systems. Payment gateways store and transmit credit card details as well as personal information which are valuable to organizations and holds monitory value. Payment domain is a target of threat agents because of the information that it handles.

Payment Gateway or any other organisation that process cardholder data needs to be PCI DSS standard compliant. PCI DSS is a standard and being compliant does not assure that security risks are treated. For the first time in the history of online fraud for credit cards knock over the in-person figures by 2016 resulting in 58% for online card fraud and 42% in-person fraud [49]. There are strict guidelines for payment processing businesses regarding the management and protection of customer sensitive data, but yet as per 2016 Verizon report, it shows 80% still fail to maintain the PCI DSS standard when processing payments [49]. Neiman Marcus [50] faced a breach in 2015 exposing 1. 1 million payment card details of customers despite the company being aligned to PCI DSS standards.

University of Cambridge has conducted a cyber risks analysis [51] worldwide by providing case studies. Denial of Service Attacks are yet a major concern in cyber security which has diverse from traditional approaches such as attacking the entire infrastructure but having focus to infrastructural components. In 2017 AWS S3 storage bucket went offline globally impacting the "*Availability*" aspect which has approximately lost 150 million dollars due to the four hours of downtime is an example that reputed cloud providers cannot guarantee to meet security objectives of data [51]. "Global data risk report" [52] by Varonis shows that 58% of organisations have not managed folder rights appropriately, which has resulted in 100,000 of folders available to the public. It is evident by now that technological advancement cannot guarantee to increase the level of security in systems and risk mitigation can be challenging due to complexities of systems and unidentified risks.

Table 7 presents payment related breaches happened in 2018 and how financial companies have been impacted due to attacks. It concludes that cyber-attacks targeting the payment processing industry has increased.

Table 7: 2018 Payment Card Breaches [53]

Company Name	Company Domain	Month	Impact and Reason	Potential Reason for breach
British Airways	Airline	September	Personal and Financial 380000 customers	Payment form script modification
Dixons Carphone	Electronics retailer	July	Personal and Financial 105000 customers	No chip and Pin protection
Ticketmaster UK	Entertainment ticket seller	June	40000 Personal and Financial	Due to a malicious software third-party application
Rail Europe	Train ticket distributor	April	Personal and Financial (The entire system was compromised)	Credit card-skimming malware in website
One Plus	Smart Phone manufacturer	January	40000 c/c details compromised	Malicious code in payment gateway

5.2 Security Risk Analysis of Payment Gateway System

Vulnerability is a weakness [5] in a IS asset and can exist in a software application, network, facility, hardware and people related to an organization. Threat agents exploit the weaknesses in the system assets. No organization can claim that the information systems are free from vulnerabilities because attackers are finding zero day vulnerabilities to exploit information systems. Therefore identifying vulnerabilities in enterprise is a continuous process. Therefore systems which handle payment data conduct vulnerability assessment each quarter as a requirement of PCI [54].

A threat agent can be anyone who uses an attack method to exploit a vulnerability in a IS system based. Objectives of a threat agent vary according to the motivation, knowledge and expertise level. Report [55] present that 90% of enterprises are vulnerable to attacks from insiders because of poor management in access privileges, complexities in technology and the capability to access sensitive data from various devices.

In the study a categorization has been introduced based on how risks will change after a migration. Figure 16 presents the Risk categorisation.

- New Risks: A risk that will not exist in In-house but will be available in cloud after the migration.
  Example: Cloud Infrastructure have shared resource pools and a threat to these pools will not exist in in-house because the IS does not exist in in-house infrastructure.
- Remaining Risks: A security risk that will exist in cloud and in-house infrastructure. The likelihood of the security risk can increase or decrease. (Risk matrix is out of scope and therefore what risks will increase and what risks will decrease will not be evaluated.)
  Example: Application level injection attack will not eliminate when the infrastructure changes. But the likelihood can change based on the defence on depth technologies used in cloud.
- Eliminated Risks: Security risks that exist in in-house infrastructure, but with never exist in cloud infrastructure.
  Example: Physical attacks towards in-house infrastructure will not be applicable in cloud because in-house employees do not have access to cloud data centre and also data is distributed.

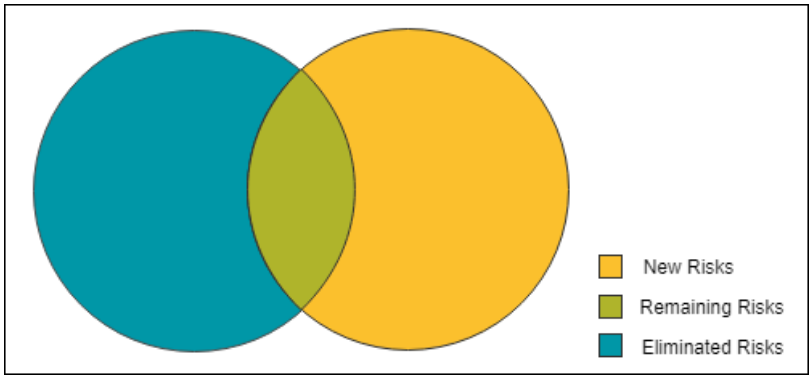


Figure 16: Risk Categorisation

5.3 STRIDE-based Threat Event and Impact Analysis

Due to the complex nature of the payment gateway, threat analysis will be conducted for IS assets that supports Order details business asset. Order details sent by the merchant contains customer name, customer DOB, customer email address, shipping address, customer address, order ID, order item, quantity and price.

Using STRIDE based asset-centric approach will be followed as ISSRM asset related consider software as an asset and attacker view on infrastructure will be considered. It is unwise to only think about the past attacks that have occurred and to check if those are potential risks in both infrastructures as there can be threats that have not yet been compromised by a threat agent. Impact due to a security risk could result in harming both business assets and supporting assets (IS assets). STRIDE categorization has previously been used by components end elements.

Table 8 presents a threat scenarios to find different risks in each infrastructure. Therefore objective is not to find the best risk scenario but give an insight of a practical example. The IS assets that exist only in-house infrastructure is considered because a threat exploit a vulnerability in a IS asset and if the chosen IS is not presented in the cloud means the risk presented for in-house will never happen on cloud environment. Therefore security risk matrix based calculations will not be needed. This should be the same when finding threats to the cloud infrastructure IS assets that supports the Order details business asset.

Three constraints were made when presenting the risk scenarios to identify unique risks.

1. Unique components of each architecture is used to form the risk scenario.
2. Business asset of the in-house and cloud-based infrastructure to a particular STRIDE category should be similar.
3. The business object of all scenarios will remain the same.

Table 8: STRIDE-based Threat Event and Impact Analysis

<table>
<tr><th>Threat Type</th><th>In-house Infrastructure</th><th>Cloud Infrastructure</th></tr>
<tr><td rowspan="2">Spoofing (SP)</td><td>IS Asset: Security guard, Server room

Vulnerability: Improper authentication mechanism in Server room

Threat Agent: An unauthorised employee,
Motivation: To steal a Backup tape for personal gain
Resources: Fake id
Expertise Level: Intermediate

Attack Method: Go to the Server room. Show a fake id and pretend to be an authorised new employee. Gain access to Server room (Server room access is only controled by security guard). Steal backup tapes of Order details.

Impact: Loss of confidentiality in Order details and loss of reliability in Backup tapes.</td><td>IS Asset: Cloud service provider , DB03

Vulnerability: Weak policies of user request handling in cloud.

Threat Agent: A contract employee,
Motivation: To sell Order details
Resources: Social engineering skills, Organization email address
Expertise Level: Intermediate

Attack Method: Send an email to Cloud service provider by a group email address. Mention about a external pentesting and request to change the firewall rules. Contract employee has spoofed the identiftiy of a legitimate user and therefore Cloud provider accepts the request to allow the traffic from a malicious ip. Scan the DB03 . Find a publicly available exploit and access Order details.

Impact: Loss of confidentiality in Order details. Tarnish the reputation of the company.</td></tr>
<tr><td colspan="2">IS Asset: Employee (Intern)

Vulnerability: Lack of security expereince and prone to social engineering

Threat Agent: A malicious employee,
Motivation: To plant a trojan for personal gain
Resources: Social engineering skills
Expertise Level: Intermediate

Attack Method: Reach an intern and pretend that the malicious employee is trying to help. Get DB credentials from the intern pretending that he is going to help. Log into the DB03 with interns credentials and execute a malicious script.

Impact: Loss of confidentiality in Order details. Loss of reliability in DB03.</td></tr>
<tr><td>Tampering (TA)</td><td>IS Asset: Backup tapes, Server room

Vulnerability: Insecurely stored Backup tapes

Threat Agent: A malicious employee,

Motivation: To destroy the Backup tapes for personal gain
Resources: A close contact with Security Guard
Expertise Level: Intermediate</td><td>IS Asset: DB03, Log server, 3rd party monitoring tool, Transmission protocol

Vulnerability: Improper security transmission protocol in 3rd party monitoring tool

Threat Agent: An attacker,

Motivation: To cover the traces of a previous attack
Resources: Knowledge about the vulnerable third-party cloud monitoring</td></tr>
</table>

	Attack Method: Access the Server room by a social engineering attack on the Security guard. Insert backup tapes into a device and modify data of Backup tapes. **Impact:** Loss of Availability in Order details. Loss of integrity in Order details. Harm the data in Backup tape.	tool Expertise Level: Intermediate /Advanced **Attack Method:** Find what is the integration software used to extract data from Log server to monitoring portal. Inject a malware to the plugin. Modify log files of Order details, so it will not be visible for monitoring. **Impact:** Loss of Confidentiality in Order details. Loss of Integrity in Order details. Loss of trust towards 3rd party monitoring tool.
Repudiation (RE)	**IS Asset:** Log server, Employee **Vulnerability:** Unauthorized alerting mechanism in Log server **Threat Agent:** A bribed employee, Motivation: Personal Gain Resources: Company Infrastructure Knowledge Expertise Level: Intermediate **Attack Method:** Go to the Server room . Plug a USB with a malware root-kit. Get Access to Log server. Remotely modify log files of Order details. **Impact:** Loss of confidentiality in Order details. Loss of integrity in Order details. Loss of trust towards Log server	**IS Asset:** Backup Storage **Vulnerability:** Non-updated access privileges to internal users **Threat Agent:** An Insider attacker, Motivation: To fulfil a grudge for degrading his position Resources: Technical knowledge about backup mechanism, Has a user account to access Log servers Expertise Level: Intermediate **Attack Method:** Login to the Log server with his valid id. Change the cron job schedule to avoid making backups. Clear the traces of his presence in the server . Logs during that period will be unavailable for later investigations. **Impact:** Loss of Availability in Order details Logs.
Information Disclosure	**IS Asset:** Server room , Backup Tapes **Vulnerability:** Insecurely stored unencrypted backup tapes **Threat Agent:** A malicious employee, Motivation: Personal gain Resources: Backup Knowledge Expertise Level: Intermediate **Attack Method:** Employee with Server room access get in. Clone the data in backup date. Access data stored in plain text. Sell Order details. **Impact:** Loss of confidentiality in Order details. Loss of trust towards data storing mechanism.	**IS Asset:** Backup Storage **Vulnerability:** Improper hardware resource decommissioning in Backup Storage **Threat Agent:** A malicious Co-Tenant, Motivation: Personal fame Resources: Backup and Recovery knowledge, Forensic Tools Expertise Level: Intermediate **Attack Method:** Co-Tenant buys Advance Forensic Tool. Execute the program and recover backup data files of DB03. Break the encryption of files to see Order details. **Impact:** Loss of Confidentiality in Order details.

	IS Asset: DB03 **Vulnerability:** Improper application level user access control **Threat Agent:** An unauthorised insider, Motivation: To view all information related to Order details (personal gain) Resources: User access control knowledge , Company employee Expertise Level: Intermediate **Attack Method:** An unauthorised insider discover that his user access role has been upgraded. Log into DB03 and retrieve Order details from DB03. **Impact:** Loss of confidentiality in Order details and loss of trust towards DB03	
Denial of Service	**IS Asset:** Heating system, Server room **Vulnerability:** Weak heat monitoring mechanism **Threat Agent:** A malicious insider, Motivation: Personal gain (grudge) Resources: Knowledge about organisation Expertise Level: Beginner **Attack Method:** Access Server room. Disable heating system. Server get over heated and malfunction. It will lead to distruptiion of service. **Impact:** Loss of availability of Order details, loss of reliability of DB03 and harm the server of DB03.	**IS Asset:** CDN Network, DB03 **Vulnerability:** Improper request routing and response handling in CDN Network [52] [53] **Threat Agent**: A malicious Co-Tenant, Motivation: Personal gain Resources: Network and Routing knowledge Expertise Level: Advanced **Attack Method:** . Co-Tenant manipulates forwarding process. Create a forwarding loop inside CDN Network (Forwarding loop attack). Forwarding loop will make one request process repeatedly. Make Unexpected massive resource consumption. These request will lead to DOS **Impact:** Loss of Availability in Order details
Elevation of Privilege	**IS Asset:** DB03, Camera **Vulnerability:** Improper USB access control **Threat Agent:** A malicious employee, Motivation: personal gain Resources: Technical knowledge and eqipment Expertise Level: Intermediate **Attack Method:** Go to the Server room. Plug in a rubber ducky to DB03 03. Get remote access to the DB03. Retrieve Order details which includes Personal information to find the revenue of the webshop from Order details. **Impact:** Loss of Confidentiality in Order details	**IS Asset:** DB03, Shared Resource Pool **Vulnerability:** Improper resource isolation in Shared Resource Pool **Threat Agent**: A malicious co tenant, Motivation: Personal gain Resources: Virtualization knowledge Expertise Level: Advanced **Attack Method:** Tenant purchase multiple VMS from the cloud provider. Get Infrastructure map and ip distribution via side channel attack. Exploit shared memory cache. 4. Get access to DB03 cache and expose Order details. **Impact:** Loss of Confidentiality in Order details. Harm the reliability of shared resource pool.

	IS Asset: phpMyAdmin interface **Vulnerability:** Misconfiguration in phpMyadmin interface of DB03 **Threat Agent:** An attacker, Motivation: To access Order details and make a copy to sell in dark web (personal gain) Resources: Knowledge of application hacking Expertise Level: Intermediate **Attack Method:** Explore vulnerabilities related to phpmyadmin**.** Explore the location of phpMyadmin interface. Upload a backdoor via dump file function and escalate privileges **Impact:** Loss of confidentiality in Order details and loss of trust in PayGate

5.4 STRIDE-based Risk Analysis

In the present, different methods are used by organisations to conduct a risk analysis. A threat and a combination of vulnerabilities in system assets that could create an impact on assets [5] create security risks. Security risk detection in early stages makes the risk treatment procedure smooth. Evolution is constant with the technological growth and adoption is needed to persist in the marketplace. Security risk ids based on different threat categories are formulated as follows in table 9

Table 9: STRIDE-based Security Risks in In-house and Cloud Infrastructure

Threat Category	**In-house Security Risks**	**Cloud Security Risks**
Spoofing	**SP. A. R1:** An unauthorized employee with a means to access Server room to steal Backup tapes of Order details by exploiting the improper authentication mechanism in Server room leading to Loss of confidentiality in Order details and loss of reliability in Backup tapes.	**SP. B. R1:** A contract employee with a means to sell Order details by using weak policies of user request handling of Cloud service provider leading to loss of confidentiality in Order details and tarnish the reputation of the company.
	SP. B. R1: A malicious employee with a means to plant a trojan to extract Order details from DB03 by exploiting database credentials of an intern with a social engineering attack leading to loss of confidentiality in Order details and loss of reliability in DB03.	
Tampering	**TA. A. R2:** A malicious employee with a means to destroy the Backup tapes by stealing a token card because of the improper access mechanism in Server room leading to loss of availability in Order details, loss of integrity in	**TA. B. R2:** An attacker with a means to cover traces of a previous attack in Log server by exploiting improper security transmission protocol used in the third party monitoring tool integrated with the Log server leading to loss of confidentiality in Order details,

	Order details and harm the data in Backup tape.	loss of integrity in Order details and loss of trust towards 3rd party monitoring tool.
	No risk scenario	
Repudiation	**RE. A. R3:** A bribed employee of In-house with a means to delete Order details logs to plant a malware to the physical device because of the misconfigured unauthorized alerting mechanism in Log server leading loss of confidentiality in Order details, loss of integrity in Order details and loss of trust towards Log server 1.	**RE. B. R3:** An inside attacker with a means to change the Cron job schedule to avoid making backups by using non-updated access privileges to internal users leading to loss of confidentiality in Order detail logs and loss of availability in Order details logs.
	No Risk Scenario	
Information Disclosure	**IN. A. R4:** A malicious in-house employee with a means to retrieve Order details to sell personal information in Dark web by using insecurely stored unencrypted backup tapes in Server room leading to loss of confidentiality of Order details, and loss of trust towards data storing mechanism.	**IN. B. R4:** A malicious Co-Tenant with a motive to sell Order details by recovering deleted files by improper hardware resource decommissioning of Backup Storage leading to loss of confidentiality in Order details.
	IN. AB. R4: An unauthorized insider with a means to view all the information related to Order details from DB03 by using the improper user access role privileges of DB03 leading to loss of confidentiality of Order details and loss of reliability in DB03 access mechanism.	
Denial of Service	**DE. A. R5:** An insider employee with a means to destroy the DB03 data store services by exploiting the heating system on the Server room not monitored leading to loss of availability of Order details, loss of reliability of DB03 and harm the server of DB03.	**DE. B. R5:** A malicious Co-Tenant with a means to cause unexpected massive resource consumption by using improper request routing and response handling in CDN leading to loss of Availability in Order details , Harm the functionality of DB03 and Harm the reputation of the PayGate organisation
	No risk scenario	
Elevation of privilege	**EL. A. R6:** A malicious insider retrieve Order details by misleading the security personal with social enginneering attack in Server room and getting	**EL. B. R6:** A malicious co-tenant get access to Order details by using improper resource isolation in Shared Resource Pool and get access to DB03 which leads to loss of confidentiality in Order details.

	access to DB03 which leads to loss of confidentiality in Order details.	
	EL. AB. R6: An attacker with a means to retrieve Order details gain access to phpMyAdmin interface of DB03 by exploiting a misconfiguration of DB03, leading to loss of confidentiality in Order details and loss of Webshop trust.	

Following two paragraphs illustrate two example scenarios from the table and provides details explanations.

Denial of service **DE. A. R5** risk exist due to a vulnerability in the in-house heating system of the Server room. The threat agent was capable to go to the Server room and damage the heating system which makes hardware in the Server room get overheated. This risk does not exist in cloud because an employee in the PayGate will never have access to go to the cloud data center. **DE. AB. R5** explains an application level risk. Data stores needs to have proper request handling to serve the legitimate request.

Elevation of privilege security risk **EL. A. R6** is an eliminated risk when the payment gateway system is migrated into the cloud. PayGate employees will not know where the data is hosted in cloud and cloud data center physical access is strictly prohibited. Therefore an employee will not be able to plug a device that could gain remote access in a cloud environment. **EL. B. R6** explains an escalation of privilege in cloud environment which is possible due to the Shared resource pools in cloud. In an in-house non-virtualized infrastructure, shared resource pools cannot be see. Therefore the risk will never exist in the in-house environment. **EL. AB. R6** is an application based security risk and the infrastructure that the application hosted will not eliminate the risk. The vulnerability [56] exist in phpMyAdmin interface will remain in in-house and cloud infrastructure.

The tables are only to illustrate some example risk scenarios. No risk scenario means that a risk scenario is not presented in the table.

5.5 Summary

Threat analysis was performed on payment gateway system hosted in in-house infrastructure and cloud infrastructure. Analysis presents how a threat event is formulated by a threat agent and threat method. The purpose of the chapter is to illustrate risk scenarios based on STRIDE. The analysis also shows what security risks will remain after migration.

6 Validation

The objective of this chapter is to evaluate the correctness of the models, and the usefulness of the EA based approach used in the study to compare security risk analysis. The chapter contains the procedure used for the validation, results of the experts' feedback and threats to validity.

6.1 Validation Procedure

The study is based on a real implementation of a payment gateway system and thus, internal users were selected based on the knowledge that they have towards PayGate as well as the experience in security risk management and cyber security. After selecting the group of sexperts, the desire towards participating in the validation process is verified to avoid faulty evaluation. Validation of the thesis started from asset identification and continued until the risk analysis.

The asset identification and security objectives of each business asset was determined by meetings conducted with the internal group including the validation and verification of the identified context. The internal group of participants were reached via Skype calls, face to face meetings and emails. During the meetings, different users based on experience were involved including business analyst, production specialist, infrastructural engineers and product owners. First few meetings were held to obtain approvals to analyse the production environment and request information related to the payment gateway such as network maps, knowledge base documents etc. Afterwards, interviews were conducted to gather the business requirements and to identify the processes. After modelling the EA and BPMN diagrams, network maps were checked by author to find if the visualisation of diagrams correspond with real implementation. Subsequently, four people were reached to verify that EA models and BPMN model are accurate. During the meetings, they made feedback on correcting the diagrams and these meetings were repeated until the experts in PayGate were satisfied with the correctness of the models.

The STRIDE threat modelling approach was used to find out the security risks of in-house and cloud infrastructure. Firstly, security risk scenarios were written to present how security risks changes based on the infrastructure change. Secondly the scenarios were validated from company experts to find out if the scenarios reflect actual threats. Afterwards, skype interviews were initiated to internal and external experts to find out the usability of EA modelling for the comparison of security risk analysis. Before each new meeting, an information session was held regarding ISSRM approach, alignment with ISO 27005 and STRIDE. The objective of background information session is to get accurate feedback during interviews and survey questions. Figure 17 presents that the validity is checked in two aspects such as correctness of models and usefulness of EA in security risk comparison. The two aspects were validated by external experts (External group) and internal experts (Internal experts).

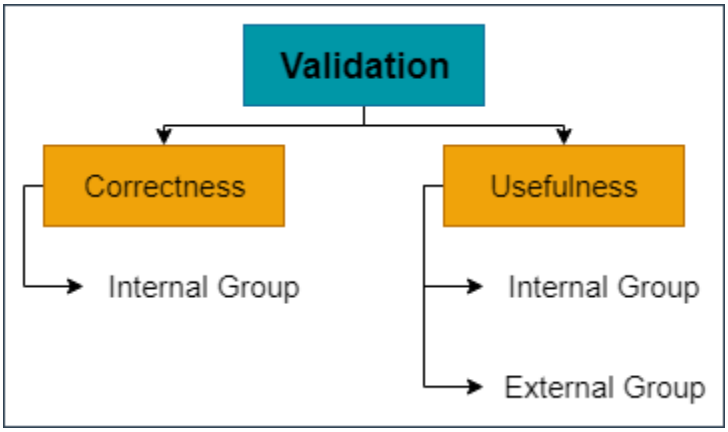


Figure 17: Validation Criteria and Participant Groups

6.2 Background of Participants

Participants for the validation was mainly selected from PayGate due to the capability they have towards validating the correctness of the model. Six people out of ten were internal from the company itself. The reason for validating the procedure via an external group is to evaluate if this approach can be used in other organisations and to which extend they this solution useful in the industry. Table 10 presents the background of the participants that were interviewed as part of the validation process.

Table 10: Background of Participants

Expert ID	**Domain of the company**	**Field of expertise**	**Designation**	**Number of experience (years)**	**Geographical region/ country**
ExpNo1	Technology	Cyber/ Security risk	Director	20	North Europe
ExpNo2	Technology	Cyber/ Security risk	Consultant	15	North Europe
ExpNo3	Technology	Cyber/ Risk/Payment	Engineer	5	North Europe
ExpNo4	Technology	Cyber/ Risk/Payment	Manager	8	North Europe
ExpNo5	Technology	Payment processing	Consultant	5	Europe
ExpNo6	Payment	Payment processing	Technical Manager	10	Europe
ExpNo7	Payment	Payment	Business Analyst	3	Europe
ExpNo8	Payment	Security	Security Engineer- PCI	5	Australia
ExpNo9	Banking	Security RM	Risk	10	Asia
ExpNo 10	IT consultation	Security	Development	7	Asia

6.3 Validation of Correctness and Usefulness

The correctness of models was validated by internal group using Skype and by face-face meetings. Here, the focus was towards validating the asset related concept of ISSRM. ExpNo6, ExpNo3, ExpNo4, ExpNo1 were mainly engaged in the model validation. The enterprise architecture was explained to the experts and discussed the need of having EA to compare security risks secondly the EA models were presented. The technology layer needed corrections because some information in network maps were outdated.

Afterword's the interdependencies and interrelationships were explained. Once when the experts confirmed the correctness of EA models, and it reflected the actual system a BPMN model of the payment transaction process was presented. Two out of six experts had knowledge about BPMN modelling. Therefore several suggestions for corrections were requested by them. Some of the comments stated by ExpNo6 and ExpNo3 were "some *tasks of the business process were missing".* ExpNo4 provided a detailed review about the errors that were against the BPMN logic which was useful to correct the remaining parts of the process. ExpNo1 checked the payment gateway system model as well as the EA model and mentioned "*To the best of my knowledge this is accurate".* When the experts agreed that BPMN models corresponded to the actual business process, the security objectives were determined by Skype discussions. By the time of the interview, they did not have a list of security objectives and therefore discussion continued until an acceptable answer was provided. Related to EA validation, ExpNo6 sent an email stating "*The architectural model corresponds completely with our current payment gateway system and matches the documentation we already have available.*" and related to BPMN diagram, "*The BPMN contains the most important business process relevant for our business. A BPMN that covers all processes would be far more complex and as a result more difficult to read*" comment was written in the email after the interview. However the study has only considered modelling only the payment transaction process therefore the comment stating about the complexity does not have any effect in the study. For remaining internal employees, the PayGate models for cloud infrastructure and in-house infrastructure were presented after providing a briefing about ISSRM and EA modelling. Afterwards, different threat scenarios based on STRIDE and security risk scenario formulations were presented to each experts. Some asked questions such as "why it is categorised as an eliminated risk and why not in in-house". Answers were provided during the discussion presenting examples.

The usefulness of the approach is validated by both internal and external groups. An introduction was made about objectives and EA modelling to external experts before the validation. Furthermore, the models were presented with a brief introduction of the ISSRM. The correctness of the models were not evaluated by external group, as a payment gateway system in another company can have a different model. Therefore, after explaining the procedure two questions were asked to evaluate the usability of the approach. Same questions were presented to the internal group via email, but did not repeat about the approach as they have already confirmed the models. Regarding the usability of the approach ExpNo1 said *"EA in Risk analysis is very impressive and it is indeed a complex task".* Since this is an interview based validation, I asked the suitability of such approach in an enterprise. The answer was *" finding resources with EA capability and analysis is rare and the modelling process can be time-consuming, but when the model is completed, this will indeed be helpful for organisations to not only to capture the changes of pre and post-migration changes but an architectural installation to the same infrastructure".* ExpNo6, the Technical Manager of PayGate has been engaged a lot in the validation process by providing feedback and accuracy checks of the models. His final comment regarding the work was "*Approach is very impressive*" Regarding the usefulness of models to compare security risk analysis of two

infrastructures , he mentioned that "*EA will be indeed useful and they have never had an idea about using EA modelling for their system to find the interdependencies and a great visualization*". ExpNo 9 and ExpNo 10 commented that "approach *is good, but there will be practical issues when modelling some systems due to over complexity*" which is acceptable.

Table 11 presents the questions given to participants of the validation. The experts were provided what is meant by 1 -10 in the scale field. Where 1 could be "Not at all", "Not useful", "Not easy at all" "highly unlikely" and "Very bad". Ten in the rating scale presented "Totally agree", "Very useful", "Very easy", "Very likely", "and Very good". (When providing the questions to experts, the explanation of the numeric values in scale was given one by one which is only relevant to the question to avoid ambiguousness. Question 1 to 4 are based on validation the correctness and question 5-7 are based on evaluating the usefulness of using EA modelling to compare security risk analysis.

Table 11: Validation Questions and Answers

Question	Scale	Average
1. How easy to understand the ISSRM approach used for Risk Management?	1-10	9.16
2. How likely do you agree with the BPMN Model?	1-10	9.75
3. How much do you think Architecture Model correspond with the actual system?	1-10	8
4. How easy it is to understand the relationship of business layer and architecture layer with the model?	1-10	8
5. How useful is the approach used in the study to identify system assets that pose threats and find security risks?	1-10	9.89
6. How likely do you think that Enterprise architecture (EA) based modelling can help to identify system assets than a BPMN diagram?	1-10	9.75
7. How you rate the suitability of the approach used in the study to compare security risk analysis using STRIDE?	1-10	7.5

6.4 Threats to Validity of Research

The research work was validated by internal and external experts. However, there can be threats which could challenge and changes the outcome of the validation results. The group of people were selected based on the experience. During the interview, background knowledge was given about ISSRM and STRIDE to have a better outcome and to avoid results based on misunderstanding. Also the payment gateway system is a real-world implementation and the accuracy of the models can be compared with the current network maps and experts feedback to find the correctness. Although, still the results can be subjective and can vary upon below facts.

- Change the group of internal and external experts
- Convincing power of the interviewer
- The mutual interest about the topic
- Level of understandability about the questions
- The correctness of the questions asked during the interview and survey
- The same question formulated in a different way

6.5 Summary

This chapter concludes the validation of the research with experts' feedback. Two user groups were involved in the validation such as internal and external. The correctness of the models that the assets were elicited and the usefulness of the procedure introduced in the work is validated. Improvements to the models were made based on the suggestions provided by the business analyst and technical product manager's viewpoint. Most of the experts provided positive feedback on the EA model based procedure used to compare security risks between two infrastructures. The company of the case study would like to continue this work and make an implementation of EA based modelling to the risk analysis process. The results presented in this section can change based on threats to validity.

7 Conclusion

Chapter 7 focuses on providing answers to the research questions, limitation of the research work done, conclusions of the work and future work which will help a researcher to continue from the finding presented.

7.1 Limitations

In this study, enterprise architecture modelling is used to show the abstract level of a real-world payment gateway system. The cloud infrastructure that was modelled using ArchiMate is generalization of the information collected from major cloud providers and the model in *Threat Modelling for Cloud Data Center Infrastructures* [33] research paper. A real-world cloud infrastructure can have different components. Also, in this research only the IaaS model is considered. But the results can be varied if the same approach is used on SaaS and PaaS.

The payment gateway system presented is modelled based on the interviews from an existing company. Payment gateway system integration might not be the same for another company therefore it is subjective.

7.2 Answers to Research Questions

In this study, the main research question is: **What procedure can be used to find differences of security risks in the in-house infrastructure and cloud infrastructure?** Before any comparison, a study about the system and the infrastructures needed. To help answer the main research question, it is broken down into three research questions. Study starts to answer:

RQ 1: What are the architectural differences between in-house infrastructure and cloud infrastructure?

The selected study is based on an actual existing payment gateway. Therefore, an analysis of the company in-house infrastructure was performed before modelling system via ArchiMate. The separation of layers and inter-dependency in ArchiMate was used to bring real-world scenario to an abstract visualization to find the connections of each components. A comparison of ArchiMate diagrams presented that there are changes in user groups, application layer and technology layer. The further analysis presented that in-house has a non-virtualized environment and manual methods for securing, while cloud architecture displayed the virtualisation components and the user group changes due to the fact that cloud provider also has access to the environment.

RQ 2: What are the business assets and supporting information system assets?

From the enterprise architecture models derived in chapter 03, payment transaction process was selected as the primary study among the four business processes that were discovered in the business layer of both infrastructures. Enterprise architecture model technology layer is an abstract view of the PayGate system. BPMN diagram did not capture all the architectural components visible even in the first level abstract. Therefore payment transaction process was modelled using BPMN language to elicit business assets from the payment transaction process. Payment transaction process in ArchiMate consisted of three sub-processes: Order Checkout, Fraud Verification and Transaction acceptance. Each was presented in the thesis separately to have better visibility. From the BPMN diagram, 6 business assets were derived. The security objectives of the business assets are presented using the confidentiality, availability and integrity properties. Security objective of each business asset was captured by conducting interviews with the Technical product manager

of PayGate to understand how important the asset is to the organisation. One business asset was choosen and the technology layer expansion was modelled again for that particular asset using ArchiMate as a second level abstraction to elicit IS assets from in-house infrastructure and cloud infrastructure. System assets of cloud which support the Order details business asset are virtualisation based technologocal components, cloud service provider. In-house infrastrcuture model consisted of security guard which supports to protect information in the server room, facilities that support to protect the secuirty objectives of order details.

RQ 3: What security risks change when a payment gateway system migrates from in in-house to cloud infrastructures?

Objective of the work is to perform a comparison of security risks in in-house and cloud infrastructure based on a threat-driven approach using STRIDE. Due to the complex nature of the study only one business asset was chosen. Second abstraction of ArchiMate level diagram is modelled to show the interdependency of one business asset with the associated technology layer. Same procedure was followed for the cloud infrastructure. IS assets that support the Order details business asset is used to find the threats and the differences of risks. Before identifying IS asset for a threat scenarios, decision was made based on:

- Risk comparison in each STRIDE category should consider only one business asset.

The reasoning behind the restrictions are, a risk can either eliminate completely, risk level increase, risk level decrease or risks can be introduced with the migration. First, only a limited number of IS assets were considered to find scenarios. The scenarios were chosen based on STRIDE categories. The results presented that security risk result can be categorise into three: new risk, eliminated risk and remaining risk. The security gap is the risk changes that can happen based on the infrastructure migration for a specific business object. This explanation shows how to find the risks in two different infrastructure and how it could be categorised based on the STRIDE approach.

Most of the risk scenarios presented in in-house are based on physical attacks. Cloud based unique risk scenarios are mostly due to the virtualisation environment. Therefore in-house physical security risks are eliminated in cloud and virtualisation based risks will be newly introduce. However this does not mean cloud has no physical attacks. But security risks by internal employees in PayGate will not be in cloud due to the distributed nature of data in cloud and cloud data centre inaccessibility. Security risks in applications that are hosted in both environments are categorised as remaining risks because code based, web application based security risks will not change depends on the infrastructure components. But the possibility of threat agent exploiting the system can be highly unlikely based on deferent defence mechanisms used in different infrastructures.

7.3 Conclusion

In organisations, business process modelling is done by a business analyst. There is an isolation between the technical user group and non-technical user group. Asset identification for RA based on BPMN diagrams might contains drawbacks such as unidentified IS assets. Therefore EA modelling is used in this study to show the mapping of business layer to Technology layer to have a better visibility of infrastructural components and the interrelationships of each layers. EA model in this work has brought an abstract of an existing scenario in a simplified manner. Asset identification is an important step as unidentified assets can carry unknown risk.

In conclusion, the analysis shows that EA model helps to identify IS assets that would have been neglected in a business process diagram. It also helps to compare and capture the differences in architecture. ISSRM is well aligned with EA models and ease asset identification. Changes to architectural components in models helps to identify IS assets that could be a threat and pose a risk to an organisation. Along with an infrastructure migration, a risk can eliminate, introduced, an existing risk can either increase or decrease. Risk has been identified for both infrastructures based on STRIDE threat approach. Validation of the work has been presented by interviewing experts in the organisation that PayGate is hosted and few external opinion about the suitability of the approach taken in the study.

7.4 Future Work

The approach used in the work to conduct a comparative security risk analysis based on two different infrastructures can be further developed as a method.

EA modelling can be used to find the interrelationships and interdependencies of business to IT layer. In present, availability of infrastructure modelling automated tools are limited. A prototype or an automated open source tool would identify the risk level of the infrastructure layer will bring this research to the next level by providing a qualitative risk gap analysis using risk matrix. Numeric value of the security risk will ease the comparison process.

There have been only limited number of research to conduct risk analysis based on enterprise architecture. Applicability of enterprise architecture in other security risk methods will improve the research area of EA modelling usability in security risk analysis. Also, same approach used in the study can be applied on a different enterprises planning to migrate to find the security risk gap using a different threat modelling approach.

8 References

[1] "12 Benefits of Cloud Computing and Its Advantages," *Salesforce.com*. [Online]. Available: https://www.salesforce.com/hub/technology/benefits-of-cloud/. [Accessed: 04-May-2019].

[2] RightScale, "RightScale 2018 State of the Cloud Report," 2018 [Online]. Available: https://www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf . [Accessed: 16- Jan- 2019].

[3] Gartner.com, "Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019," *Gartner* , 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras. [Accessed: 19-Apr-2019].

[4] "Network Security Infrastructure Report," *Netscout*, 2018. [Online]. Available: https://www.netscout.com/report/. [Accessed: 19-Apr-2019].

[5] R. Matulevičius, *Fundamentals of secure system modelling*. Cham: Springer, 2017.

[6] R. M. Blank and P. D. Gallagher, "Guide for conducting risk assessments," 2012.

[7] "Managing Risk in the Cloud," in *Cloud Computing Security*, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742: CRC Press, 2016, pp. 79–86.

[8] "PCI DSS Quick Reference Guide," pp. 1–40.

[9] H. Bahtit, B. Regragui, "Risk Management for ISO 27005 Decision support," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 2, 2013.

[10] V. Agrawal, "A Framework for the Information Classification in ISO 27005 Standard," *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, 2017, pp. 264-269.

[11] "IT-Grundschutz - Information Security Management." [Online]. Available: https://www.tuvit.de/en/services/information-security-management/it-grundschutz. [Accessed: 26-Dec-2018].

[12] "ISO/IEC 27005:2018(en), Information technology — Security techniques — Information security risk management." [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en. [Accessed: 26-Dec-2018].

[13] M. S. Lund, B. Solhaug, and K. Stølen, "*Model-driven risk analysis : the CORAS approach*", Springer, 2010.

[14] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann and R. Wieringa, "An integrated conceptual model for information system security risk management supported by enterprise architecture management", Software & Systems Modeling, 2018.

[15] F. Vraalsen, T. Mahler, M.S. Lund, I. Hogganvik, F. Braber, K. Stølen, "Assessing Enterprise Risk Level: The CORAS approach," in *Advances in Enterprise Information Technology Security*, IGI Global, 1AD, pp. 311–333.

[16] CLUSIF, "MEHARI-2010-Reference-Manual of Mehari 2010 Knowledge Base" 2006.

[17] N. Mayer, P. Heymans, and R. Matulevičius, (2007). "Design of a Modelling Language for Information System Security Risk Management", *1st International Conference on Research Challenges in Information Science*, 121-132., 2007

[18] C. Alberts, A. Dorofee, J. Stevens and C. Woody, "Introduction to the OCTAVE® Approach", Carnegie Mellon University, 2003 [Online]. Available: https://www.itgovernance.co.uk/files/Octave.pdf. [Accessed: 29- Dec- 2018]

[19] A. Tewari, "Comparison between ISO 27005, OCTAVE & NIST SP 800-30 - SISA Information Security", SISA Information Security. [Online]. Available: https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30/. [Accessed: 29- Dec- 2018]

[20] Z. Jourdan, R. Rainer, Jr., T. Marshall and F. Ford, "An Investigation Of Organizational Information Security Risk Analysis", Journal of Service Science (JSS), vol. 3, no. 2, 2010.

[21] N. Al-Safwani, S. Hassan, and N. Katuk, "A Multiple Attribute Decision Making for Improving Information Security Control Assessment," *Int. J. Comput. Appl.*, vol. 89, no. 3, pp. 19–24, Mar. 2014.

[22] O. Altuhhova, R. Matulevičius, and N. Ahmed, "An Extension of Business Process Model and Notation for Security Risk Management," *Int. J. Inf. Syst. Model. Des.*, vol. 4, no. 4, pp. 93–113, 2013.

[23] M. Välja, 'Improving IT Architecture Modeling Through Automation : Cyber Security Analysis of Smart Grids', PhD dissertation, Stockholm, 2018.

[24] P. Koning, I-to-i.nl, 2017. [Online]. Available: https://www.i-to-i.nl/wp-content/uploads/2017/04/Risk-Modeling-With-ArchiMate-Pascal-de-Koning-mrt2017.pdf. [Accessed: 18- Jan- 2019]

[25] Opengroup.org, "ArchiMate® 3.0.1 Specification." [Online]. Available: http://pubs.opengroup.org/architecture/ArchiMate3-doc/chap03.html. [Accessed: 14-May-2019].

[26] T. Sommestad, M. Ekstedt, and H. Holm, "The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures," *IEEE Syst. J.*, vol. 7, no. 3, pp. 363–373, Sep. 2013.

[27] H. Holm, K. Shahzad, M. Buschle and M. Ekstedt, "P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," in IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 6, pp. 626-639, 1 Nov.-Dec. 2015.

[28] Foreseeti, "SecuriLang Reference Manual -." [Online]. Available: https://community.securicad.com/securilang-reference-manual/. [Accessed: 18-Mar-2019].

[29] H. Shafiq, K. Asif, A. Shabir, R. Ghulam, and I. Sajid, "Threat Modelling Methodologies: A Survey," 2014. [Online]. Available: https://www.academia.edu/29215191/threat_modelling_methodologies_a_survey. [Accessed: 18- Jan- 2019]

[30] Shostack A., Threat modeling: Designing for Security. Wiley, 2014.

[31] A. Obot, "Security Risk Management of E-commerce Systems", University of Tartu, 2018.

[32] F. Innerhofer-Oberperfler and R. Breu, "Using an Enterprise Architecture for IT

Risk Management.” ISSA (2006).

[33] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, “Threat modeling for cloud data center infrastructures,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10128 LNCS, pp. 302–319.

[34] K. Singh and J. Aggarwal, "Fear of cloud computing: Identifying risks involved using STRIDE", Troindia.in, 2017. [Online]. Available: http://troindia.in/journal/ijcesr/vol4iss11/23-30.pdf. [Accessed: 02- Feb- 2019]

[35] R. Matulevičius, A. Norta, C. Udokwu, and R. Nõukas, “Security risk management in the aviation turnaround sector,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10018 LNCS, pp. 119–140, 2016.

[36] J. Janulevičius, “Method of Information Security Risk Analysis for Virtualized Systems,” Vilnius Gediminas Technical University, pp. 1–112, 2016.

[37] I. Tovstukha, “Management of Security Risks in the Enterprise Architecture using ArchiMate and Mal-activities.” University of Tartu, 2017.

[38] W. Engelsman, B. Christophe Feltus, S. González Paredes, D. Diligens Jim Hietala, T. Open Group Henk Jonkers, and B. Sebastien Massart, “Modeling Enterprise Risk Management and Security with the ArchiMate ® Language,” 2015.

[39] Alexsoft, “How to integrate payment gateways and choose a provider". 2019, [Online]. Available: https://www.altexsoft.com/blog/business/how-to-choose-and-integrate-payment-gateway-online-payments-transaction-processing-and-payment-gateways-providers/. [Accessed: 20-Apr-2019].

[40] P. Smirnoff, “Understanding Hardware Security Modules (HSMs).” 2017 [Online]. Available: https://www.cryptomathic.com/news-events/blog/understanding-hardware-security-modules-hsms. [Accessed: 08-May-2019].

[41] C. Wueest, M. Ballano Barcena, and L. O’brien, “Mistakes in the IaaS Cloud could put your data at risk.”, Symantec, 2015.

[42] Zubair Lone and Aaqib Iqbal Wani, “A Survey of Security Issues and Attacks in Cloud and their possible defences,” 2017.

[43] T. Erl, R. Puttini, and Z. Mahmood, *Cloud computing : concepts, technology, and architecture* (1st ed.), Prentice Hall Press, 2013.

[44] T. Shinder, “What Does Shared Responsibility in the Cloud Mean?,” *Microsoft Azure*, 2018. [Online]. Available: https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/. [Accessed: 28-Dec-2018].

[45] H. Jonkers, M. M. Lankhorst, H. W. L. Ter Doest, F. Arbab, H. Bosma, and R. J. Wieringa, “Enterprise architecture: Management tool and blueprint for the organisation,” *Inf Syst Front*, vol. 8, pp. 63–66, 2006.

[46] “44 U.S. Code § 3542,” *Legal Information Institute*. [Online]. Available: https://www.law.cornell.edu/uscode/text/44/3542. [Accessed: 29-Dec-2018].

[47] Linda Pesante, “Introduction to Information Security,” 2008. [Online]. Available: https://cyberdivision.net/2017/10/09/introduction-to-information-security/. [Accessed: 29-Dec-2018].

[48] Statista, “Digital buyers worldwide 2021 | Statistic.” [Online]. Available: https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/. [Accessed: 05-Jan-2019].

[49] Verizon, “PCI Compliance Report.” [Online]. Available: http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf. [Accessed: 29-Dec-2018].

[50] J. Vijayan, “After Target, Neiman Marcus breaches, does PCI compliance mean anything? | Computerworld.” 2014. [Online]. Available: https://www.computerworld.com/article/2486879/data-security/after-target--neiman-marcus-breaches--does-pci-compliance-mean-anything-.html. [Accessed: 29-Dec-2018].

[51] A.W. Coburn, J. Daffron, A.Smith, J. Bordeau, É.Leverett, S. Sweeney, T. Harvey, "Cyber Risk Outlook 2018.", Centre for Risk Studies, University of Cambridge, 2018

[52] Varonis Data Lab, “2018 Global data risk report," 2018 [Online]. Available: https://info.varonis.com/hubfs/2018 Varonis Global Data Risk Report.pdf. [Accessed: 02- Jan- 2019]

[53] L. Irwin, “Lessons to learn from recent payment card breaches - IT Governance Blog,” [Online]. Available: https://www.itgovernance.co.uk/blog/pci-dss-lessons-to-learn-from-recent-payment-card-breaches. [Accessed: 29-Dec-2018].

[54] SecurityMetrics, "2017 SecurityMetrics Guide To PCI DSS COMPLIANCE", 2017 [Online]. Available: https://www.securitymetrics.com/static/resources/orange/2017-securitymetrics-pci-guide.pdf. [Accessed: 06- Feb- 2019]

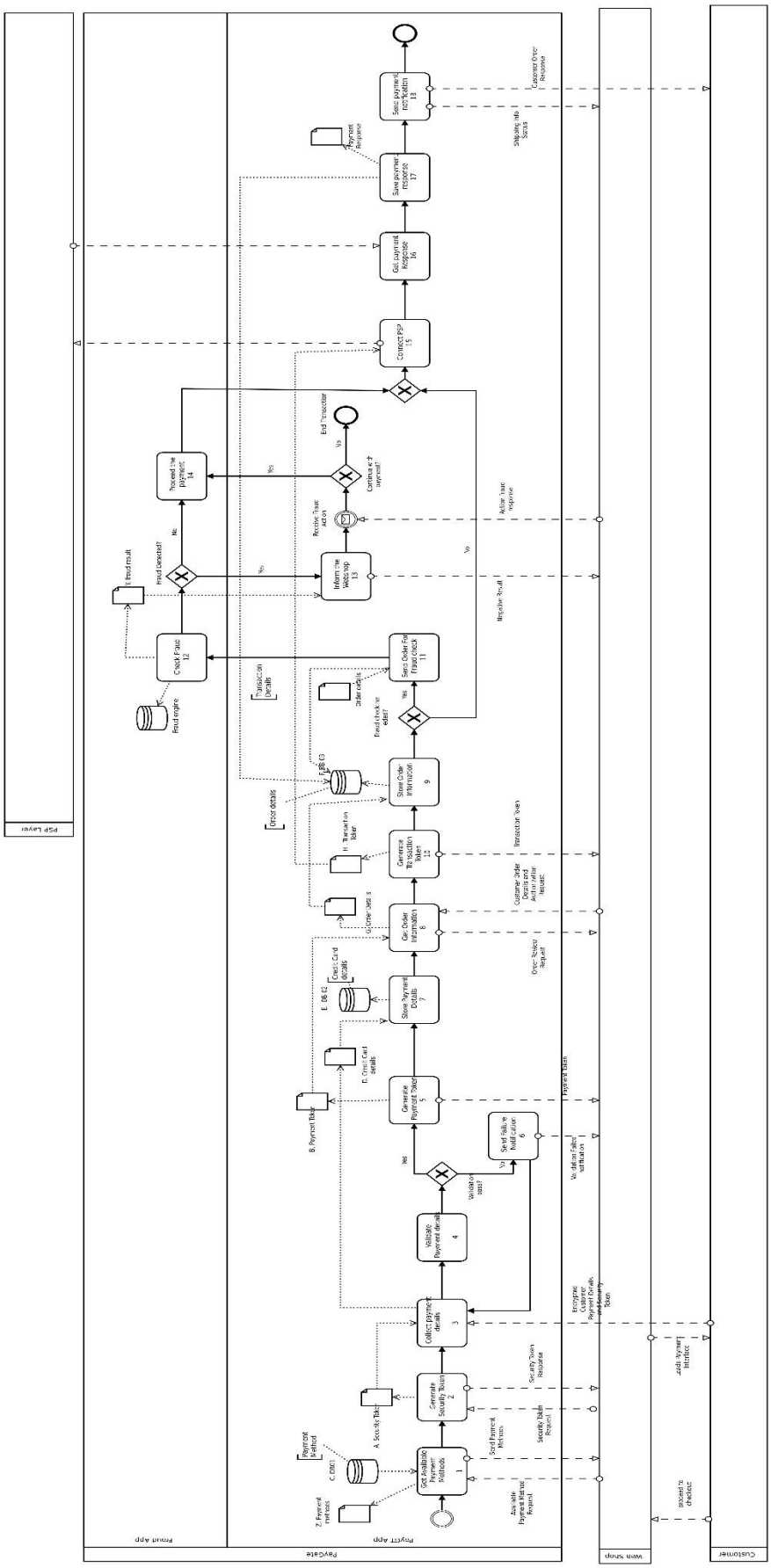
[55] Cybersecurity Insiders, "Insider Threats", CA Technologies, 2018 [Online]. Available: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf. [Accessed: 02- Jan- 2019]

[56] S. Dhar, “Code Execution and Privilege Escalation – Databases.” 2016 [Online]. Available: https://resources.infosecinstitute.com/code-execution-and-privilege-escalation-databases/#gref. [Accessed: 05-May-2019].

[57] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, “Threat Modeling for Cloud Data Center Infrastructures,” 2016. [Online]. Available: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=921695. [Accessed: 29-Dec-2018].

[58] P. Mell and T. "Grance, Cloud Computing Security Essentials and Architecture" The NIST Definition of Cloud Computing: National Institute of Standards and Technology, Information Technology Laboratory, 2018.

Appendix A: Payment Transaction Process



I. License

Non-exclusive licence to reproduce thesis and make thesis public

I, Pubudini Gayanjalie Dissanayake,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

A Comparison of Security Risk Analysis in the In-house IT Infrastructure and Cloud Infrastructure for the Payment Gateway System,

supervised by Hayretdin Bahsi PhD, Raimundas Matulevičius PhD

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Pubudini Gayanjalie Dissanayake

16/05/2019