UNIVERSITY OF TARTU
Institute of Computer Science
Cybersecurity Curriculum

Affia, Abasi-amefon Obot

Security Risk Management of E-commerce Systems

Master's Thesis (30 ECTS)

Supervisor(s): Raimundas Matulevičius Ph.D

Tartu 2018

Security Risk Management of E-commerce Systems

Abstract:

Security risk management is a vital part of any system development including e-commerce systems. As many people rely on these e-services, its inadequate security measures can be experienced, causing great losses to both businesses and customers. This thesis research work proposes a procedure that targets e-commerce system security and suggests the application of a threat-driven approach to security risk management by analysing an e-commerce system Webshop as a case study.

This approach provides a useful assessment of the security risk management procedure that is validated by experts in the field. It not only identifies evolving threats to e-commerce systems but allows for a structured flow in security risk management. The risk management process is documented and reported in such a way that is easily understandable by concerned stakeholders of the e-commerce system.

Keywords:

Threat analysis, E-commerce, BPMN, ISSRM, STRIDE, Threat modelling.

CERCS:

T120 – Systems engineering, computer technology

Elektrooniliste kaubandussüsteemide turvariski juhtimine

Lühikokkuvõte:

Turvariski juhtimine mängib iga süsteemi väljatöötamisel olulist rolli ja see kehtib ka elektrooniliste kaubandussüsteemide kohta. Kuna paljud inimesed kasutavad neid teenuseid, võivad nad kokku puutuda ebaadekvaatsete turvameetmetega ja see on kahjulik nii äritegevusele kui klientidele. Antud lõputöö toob uurimistöö tulemusena välja elektrooniliste kaubandussüsteemide toiminguid, mis on suunatud turvariskide vähendamisele, uurides ja analüüsides Webshop poodi.

Käsitletav meetod käsitleb turvariski juhtimise strateegiate hindamist, olles selle eriala ekpertide poolt kinnitatud ning ei käsitle mitte ainult elektrooniliste kaubandussüsteemide potensiaalsete ohtude määratlemist, vaid tagab ka turvariski juhtimise struktureeritud kulgemise. Turvariski juhtimise protsess on esitatud sellisel kujul, et ta on asjakohastele elektrooniliste kaubandussüsteemide osanikele arusaadav.

Võtmesõnad:

Riskianalüüs, elektrooniline kaubandus BPMN, ISSRM, STRIDE, riski modelleerimine.

CERCS:

T120 – Süsteemitehnoloogia, arvutitehnoloogia

Table of Contents

Terms and Notations 8
1 Introduction 9
1.1 Motivation 9
1.2 Scope 9
1.3 Problem Description 10
1.4 Research Question 10
1.5 Contribution 11
1.6 Structure 12
2 Literature Review and Thesis Background 13
2.1 Security Risk Management Standards 13
2.2 ISSRM Security Risk Management Methodology 14
2.2.1 Domain Model 14
2.2.2 ISSRM Process 15
2.1 Previous Work on Security Risk Management 15
2.1.1 Analysis of Digital Security Threats in Aviation Sector 16
2.1.2 Securing Airline Turnaround Processes using Security-Risk Oriented Patterns 17
2.1.3 Online Banking Security Analysis based on STRIDE Threat Model 17
2.2 Model Representation for Security Risk Management 18
2.3 Threat-driven Perspective to Security Risk Management 18
2.4 Summary 21
3 Assets in E-commerce System 22
3.1 The E-commerce System and its Components 22
3.2 Security Objectives in an E-commerce System 23
3.3 The E-commerce Order Fulfilment Business Process 23
3.3.1 Product Catalog 24
3.3.2 Shopping Cart 24
3.3.3 Payment Process 24
3.3.4 Shipping 26
3.4 Security Assets in an E-commerce System 26
3.5 Summary 31
4 Security Risk in E-commerce Systems 32
4.1 E-commerce Risk Landscape 32
4.2 Vulnerabilities in E-commerce Systems 33
4.3 Security Threats in E-commerce Systems: STRIDE 35

4.4 Security Impact of Threats on E-commerce Systems 36
4.5 Summary 40
5 Security Risk Treatment 41
5.1 E-commerce System Requirements Definition 41
5.2 Security Requirements Elicitation 41
5.3 Security Requirements Model 43
5.4 Technical Security Countermeasure Selection 45
5.5 Summary 49
6 Security Risk Measurements 50
6.1 Security Risk Metrics 50
6.2 Security Risk Metric Example 50
6.3 Security Trade-off Analysis 53
6.4 Summary 58
7 Validation of Security Risk Management Procedure 59
7.1 Expert Background 59
7.2 Description of Validation Procedure 60
7.3 Results of Validation Procedure 61
7.3.1 Validation of Asset-related Concepts 61
7.3.2 Validation of Risk-related Concepts 61
7.3.3 Validation of Risk Treatment-related Concepts 62
7.4 Threats to Validity 63
7.5 Summary 64
8 Summary of Work 65
8.1 Limitations of Research 65
8.2 Answer to Research Questions 65
8.3 Concluding Remarks 67
8.4 Proposals for Future Work 68
9 References 69
Appendix 72
I License 72

Table of Figures

Figure 1: ISSRM Domain Model [20] 15

Figure 2: ISSRM Process [20]........ 16

Figure 3: Threat-driven Approach........ 19

Figure 4: Value Chain 24

Figure 5: Product Catalog Process 25

Figure 6: Shopping Cart Process 25

Figure 7: Payment Process 27

Figure 8: Shipping Process........ 28

Figure 9: E-commerce Webshop Business Process 30

Figure 10: Security Requirements Application to E-commerce Webshop Business Process........ 46

Figure 11: Security Requirements Application to the Carry Out Login Procedure of Webshop........ 47

Figure 12: Risk reduction level vs. Business Asset Value........ 56

Figure 13: Risk Reduction Level vs. Cost of Countermeasure 57

Figure 14: Cost of Countermeasure vs. Business Asset Value 57

Figure 15: Concept of Expert Background for Validation........ 59

List of Tables

Table 1: Top Retail Data Breaches in Retail [3] 33
Table 2: Taxonomy of Vulnerabilities 35
Table 3: STRIDE Approach for E-commerce System Threats 37
Table 4: STRIDE-based Security Risk Impact Analysis 39
Table 5: STRIDE-based Security Requirements Elicitation 42
Table 6: Security Countermeasure Suggestion 48
Table 7: Business Asset Value 51
Table 8: Security Objective Metrics 51
Table 9: Threat Likelihood 51
Table 10: Vulnerability Level of System Assets 52
Table 11: Cost of Countermeasure Metric 52
Table 12: DR1 Security Risk Reduction Level Metric 54
Table 13: Risk Metrics Before and After Risk Treatment 55
Table 14: Determining Risk Priority 58

Terms and Notations

Term	Description
CWE	Common Weakness Enumeration
COBIT	Control Objectives for Information and Related Technology
ISACA	Information Systems Audit and Control Association
NIST	National Institute of Standards and Technology
BPMN	Business Process Modelling Notation
ISSRM	Information System Security Risk Management
CAPEC	Common Attack Pattern Enumeration and Classification
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges
OWASP	Open Web Application Security Project
PSP	Payment Solutions Provider
PCI DSS	Payment Card Industry Data Security Standard
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
GQM	Goal Question Method
RQ	Research Question
ST	Spoofing Threat
TT	Tampering Threat
RT	Repudiation Threat
IT	Information disclosure Threat
DT	Denial of service Threat
ET	Elevation of privilege Threat
SR	Spoofing Risk
TR	Tampering data Risk
RR	Repudiation Risk
IR	Information disclosure Risk
DR	Denial of service Risk
ER	Elevation of privilege Risk
SReq	Security Requirements

1 Introduction

1.1 Motivation

The ease that an e-commerce system provides ensures that a large volume of customers will continue to use these systems with growing orders made electronically and delivery carried out with no geographical limitations. These systems enhance normal business flows as now, e-commerce transactions occur between businesses, customers, businesses and customers, and so on. A survey of customer's online shopping habits reveals that more than 5,000 customers will make at least two online purchases within a three-month period [10]. According to this survey, compared with a 47% purchases in 2014 and 48% in 2015, customers now carry out 51% of their purchases online [10]. With the advantage of the possibilities of online purchases, businesses which decide to choose the e-commerce option typically show a rise in sales [10]. However, the ease introduced by e-commerce solutions has also been accompanied by severe cyber threats to the system. Sensitive information is now being generated, collected, stored, transmitted, and manipulated on technologies and through processes that may not have adequate security capabilities. Customers now fear the loss of financial data and e-commerce systems fear the financial losses as well as other losses associated with security risks. With these security concerns, a consistent analysis of threats that pose security risks, as well as a continuous process into the treatment of these risks. This paper seeks to provide a structured and logically illustrated approach to continuous threat analysis and security risk management specific to the e-commerce domain. This approach will also facilitate participation between business professionals (who want to participate in a more effective way in building, using and managing e-commerce systems), and the IT professionals (who seek to work more effectively with the business professionals when building and maintaining their e-commerce systems).

1.2 Scope

This thesis work illustrates how security risk can be managed in an e-commerce system. The following section provides specific boundaries/scope of the thesis work.

Risk management is a general concept, applied to many areas and domains of life, not just in Information Systems. Risk management is defined as the "*coordinated activities to direct and control an organization with regard to risk*" [18]. Security risk management, on the other hand, has its focus on risks that occur through malicious intent as the word security here, defined by [8], is "*the degree to which malicious harm is prevented, detected, and reacted".*

Security risk management still covers a wide range of systems of which an e-commerce system is one. This work will focus on the Information Systems category. An information system, according to [37] is a "*system for dissemination of data between persons - potentially, to increase their knowledge".* Data in an e-commerce system could be facts about objects on sale, or customer name, age, address, telephone number, account number, payment card number, or product transactions. E-commerce allows information to flow between organizations and external customers, suppliers, and competitors with the aim of carrying out a business transaction.

E-commerce is generally a buzzword for the use of the internet to facilitate transactions in sale and payment of goods and services between parties. These parties can include a number of categorizations such as Customer-to-Customer, Business-to-Customer, Business-to-Business, Business-to-Government, and so on. However, for the purpose of this thesis work, the e-commerce system referred to and focused on, is the Business to Consumer type. This category consist of a number of business processes that together achieve the goal of e-commerce. The business process that will be further considered is the order management process in an online Business-to-Customer (B2C) store.

An e-commerce system is one comprising several components and interactions with other systems. This system comprises of software, hardware, processes, and services, some of which could be third-party. Usually, Merchants of e-commerce systems engage third parties in carrying out services to support the e-commerce system as commonly seen with Payment Solution Providers (PSPs), and Shipping Companies. However, security risk management in this paper is only carried out on aspects that are directly under the control of the Business to Customer e-commerce system. These third-party agents may be instantiated in models for risk illustration but risk mitigations are carried out independent of these third-party systems.

The STRIDE approach, is used to find possible attacks on the e-commerce scenario may come to play. This thesis research will use STRIDE as a threat modelling method not just for threat elicitation but as a structure to continue the security risk analysis and treatment phase.

1.3 Problem Description

The benefits of e-commerce encourage businesses to seek an e-commerce solution for transactions. Thus, e-commerce systems are increasingly being built and business sensitive assets are now used on technologies and processes that may not be secure. These technologies and processes pose threats, evolving over time, to the e-commerce system. As such, an enhancement to the procedure of following risk management is needed. This should allow for continuous threat analysis and management of the resulting risk, applicable for the phases of an e-commerce system development.

1.4 Research Question

For the purpose of this research work, the following main research question is proposed.

What procedure can be used to carry out risk management with a focus on evolving threats to e-commerce systems?

To be more specific, the main research question is broken up into three areas;

1. Identification of business context, discussed in Chapter 3 of this thesis work.
2. Threat modeling and risk analysis, discussed in Chapter 4 of this thesis work.
3. Risk treatment procedures, discussed in Chapter 5 and 6 of this thesis work.

These research areas are further developed into research questions;

RQ1: How can relevant assets for an e-commerce system be identified?

Answering this question reveals how assets that need to be secured in an e-commerce system can be identified and also reveals the importance of this identification to the risk management process of an e-commerce system.

RQ2: What are the security threats as well as its resulting risk to an e-commerce system? After asset identification in **RQ1**, recognizing system vulnerabilities, threats and the resulting impacts and risks are useful in security risk management.

RQ3: What are the risk treatment procedures in risk management for an e-commerce system?

This question will help to understand how to tackle the security issues raised in **RQ2.** After the recognition of threats and the impact of these threats, a decision should be made on treating the security risk. Answers to this question will outline the risk treatment procedures needed for security risk management.

The answers to these research questions do not provide a measure for "perfect" security, but instead illustrates a procedure that is beneficial to security risk management in an e-commerce system.

1.5 Contribution

This work follows a design-science research method for information systems research that deals with the development of the theories and artefacts to help organisations address business needs. With information from existing knowledge base, new artefacts can be developed and evaluated, serving as a meaningful addition [15].

This thesis contributes to the security risk management research society by applying a structured threat-driven approach to the information systems security risk management (ISSRM) domain model for an e-commerce system. It provides an understanding of its alignment to ISSRM methodology expressing assets, threats, risks and risk treatment concepts using modelling and analytical tools. The applicability of this approach is shown in an illustrative example of an order management process in a Webshop. This proposal will allow a structured flow from threat analysis to the resulting risk management with focus on a threat-driven approach. The answers to its research questions will create a viable and engaging procedure to risk management in e-commerce systems. This thesis research analysis will be useful to both technical and non-technical audiences such as business analysts, business stakeholders, system developers, system analysts, and cybersecurity experts.

The product of this research work will be subjected to evaluation by experts in the e-commerce industry as well as experts in related Information Systems. Concepts used in this research such as risk management methodologies and modelling concepts have been previously demonstrated by academic researchers including Raimundas Matulevičius and Olga Altuhhova.

1.6 Structure

The thesis work is organised into eight chapters;

Chapter 1 introduces the thesis research, including its motivation, scope, problem description and research goal for the thesis work.

Chapter 2 progresses from a discussion on security standards that support ISSRM approaches, to the use of ISSRM and STRIDE in previous research on security threat analysis and risk management. The STRIDE threat-driven approach, an integral part of this thesis research will be discussed.

Chapter 3 highlights the security assets that require protection from malicious activities and how can be elicited from the business process of the e-commerce system.

Chapter 4 deals with the vulnerabilities, a characteristic of the system assets discussed in the previous chapter and progresses to illustrate how threats can be modelled from these assets leading to the impact on the system that results in a security risk.

Chapter 5 focuses on risk treatment-related concepts including security requirement elicitation in order to mitigate risk.

Chapter 6 deals with risk measurements including some risk trade-off analysis carried out as simultaneously treating all risk is unrealistic.

Chapter 7 outlines the expert's validation procedure for the STRIDE based approach to security risk management used.

Chapter 8 highlights the conclusion of the thesis research, its contribution, answers to the research questions posed by the thesis work, and a discussion on avenues for future work.

2 Literature Review and Thesis Background

The area of security risk management research is not novel but rather a long-standing continuous tradition. This chapter serves as a literature review, introducing security risk management approaches and its regard to systems related to e-commerce as well as more insight into the research design used in this thesis work. Previous work done on the use of ISSRM, STRIDE and modelling techniques for security risk management is discussed, providing ways of understanding the security need, security threats and the risk management process.

2.1 Security Risk Management Standards

A number of standards to manage security risks in information systems of which e-commerce is one. Security standards define guidelines suitable for security risk management which, as a discussion in this section, will first cover an overview of the ISO 2700x series [18], NIST publications and the Risk IT framework, and other standards such as PCI DSS and IT-Grundschutz.

The first standard is the ISO2700x standards which for example has the ISO/IEC 27005:2011, applicable to many organisations, and provides a set of guidelines and techniques for information security risk management [19]. It also supports the concepts, models, processes and terminologies of information security risk management specified in the ISO/IEC 27001 and ISO/IEC 27002 and aids the satisfactory implementation of security following a risk management approach.

The NIST (National Institute of Standards and Technology) has published a set of standards that address security risks in information system as seen in NIST SP 800-39 [11] and NIST SP 800-30 [12]. The NIST SP 800-39 serves as a guide for an organisation-wide program for information security risk management using a multi-tiered approach having an organizational tier, business process tier and information systems tier [11]. This risk management approach follows four components to manage risk (1) frame risk; (2) assess risk; (3) respond to risk; with these components being addressed in NIST SP 800-30 [12]. This standard guides the communication between the risk assessment process and other organizational risk management processes. The NIST publication 200 includes within it, a mixed set of security requirements for planning, risk assessment, technical requirements, and even physical environment protection requirements.

The RiskIT framework is part of ISACA's initiative, based on a set of guiding principles based on principles, dedicated to helping enterprises manage IT-related risk [17]. This framework complements ISACA's COBIT by providing a more comprehensive set of good practices to identify, govern and manage IT risk for business-driven IT-based solutions and services. Thus, the Risk IT Framework enhances risk management for organisations that adopt COBIT as their IT governance framework. The Risk IT framework bridges the gap between generic risk management standards such as the ISO and domain-specific frameworks providing a comprehensive view that enables enterprises to understand and manage significant IT risk types [17].

One other standard particularly relevant for e-commerce systems is the Payment Card Industry Data Security Standard (PCI DSS) standard is more of a compliance standard specific to financial and e-commerce systems [29] and applies to those processing payment card data for transactions. As e-commerce systems use payment cards for transactions, the system and third-party connections must be PCI-DSS compliant [29]. This standard lists guidelines that should be followed in order to be compliant as a failure to meet the standard inevitably leads to steep fines, a damaged reputation and loss of customers. Thus, this should be considered during security risk management. These guidelines include Public Key selection, the use of encryption and digital certificates, and choosing PCI compliant hosting provider.

Other standards exist such as the IT-Grundschutz (a German standard for security management methods). However, discussions on the standards for security risk management serve as a basis to define security risk management methodologies to be used in specific domains of information systems. Methodologies will combine the principles proffered by the standards discussed in a perspective and guidance for security procedure within the specific domain.

2.2 ISSRM Security Risk Management Methodology

A security risk management methodology is an analytical procedure that follows security standards to identify valuable system assets, stakeholders and operations, as well as the risk levels of undesirable events with the aim of providing logic and guidance for identifying and implementing solutions for the specific risk situation and mitigation strategies. In order to achieve this, methodologies have been developed [20]. For this reason, the ISSRM methodology [6], its domain model, its concepts, relationships, metrics and risk management process will be discussed.

2.2.1 Domain Model

A domain model is developed through a survey of security and security risk management related standards and methods, introduced to guide activities of risk management by the people working on them [6]. The domain model for ISSRM characterizes three key concepts: the *asset-related* concepts, the *risk-related* concepts and the *risk treatment-related* concepts: marked correspondingly as blue, orange and green in Figure 1.

The *asset-related* concepts describe the assets that need to be protected according to the security need of the system. The *business asset* is defined as any information, process or skill necessary for achieving the business objectives of a system with its security need characterised by *security criterions* of *confidentiality, availability, and integrity* and wholly supported by *IS assets*.

The *risk-related* concepts demonstrate how *risks* are reached through a combination of *threats* (consisting of *threat agents* that use *attack methods* to execute threats) exploiting on one or more *vulnerabilities* that are a characteristic of *IS assets*, leading to a considerable impact that harms *assets* and negates the *security criterions* of the *business assets*.

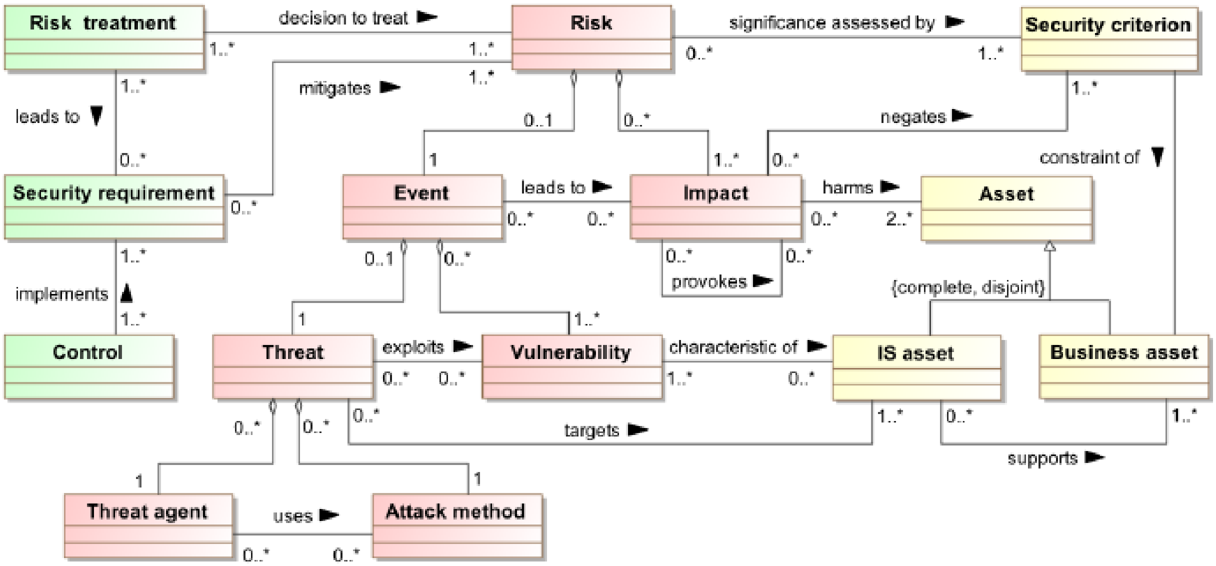


Figure 1: ISSRM Domain Model [20]

The *risk treatment-related* concepts include decisions to treat risk based on analysis done on *controls* that implement *security requirements* which serve to mitigate risk and thus refine the risk treatment process.

2.2.2 ISSRM Process

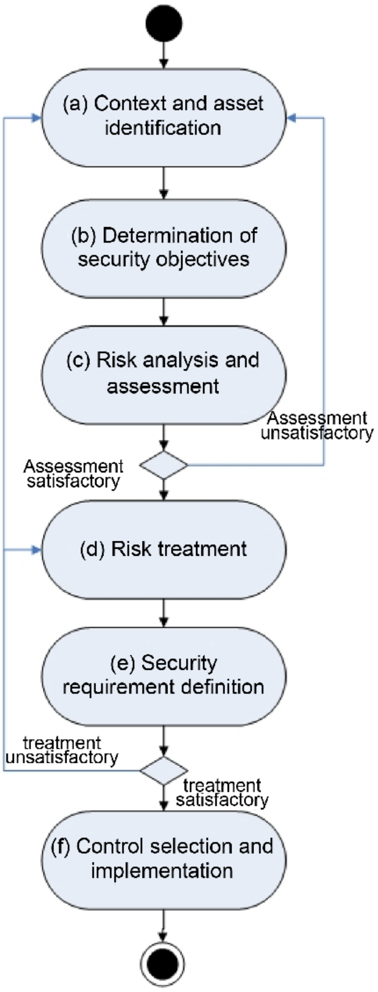
This process describes activities that are necessary for security risk management as seen in Figure 2. The first step is the *context and asset identification* which analyses the organisation, its environment, as well as its assets. Next, the *security objective determination* based on the *confidentiality, integrity and availability* of each business asset is carried out. The third step is *risk analysis and assessment* to identify and estimate risks. After these stages, in case of an unsatisfactory assessment for reasons such as missing assets, or a change in scope, these three processes can be iterated.

The *risk treatment* stage includes decisions to treat the security risk developed. The *security requirements definition* stage is necessary to state security conditions that need to be true in order to achieve security of the system based on known risk situations. In the event of unsatisfactory treatment results, there could be a need to iterate from the beginning of the ISSRM process, or from the *risk analysis and assessment* stage.

The *security selection and implementation* stage define specific technologies needed to be implemented within the system.

2.1 Previous Work on Security Risk Management

The use of the ISSRM methodology and its Domain Model for risk management and as a reference to the enhancement of risk management procedures is not a new topic, as there has been previous research works done on this. This work is based on the notion that ISSRM and its Domain Model is a reliable methodology that can be used in a security risk management process and as a guiding reference when developing concepts that enhance the security risk management process.



(a) Context and asset identification
(b) Determination of security objectives
(c) Risk analysis and assessment
Assessment unsatisfactory
Assessment satisfactory
(d) Risk treatment
(e) Security requirement definition
treatment unsatisfactory
treatment satisfactory
(f) Control selection and implementation

Figure 2: ISSRM Process [20]

This work is also based on the notion that the STRIDE method is a viable method for threat analysis in the security risk management process. Three research works are discussed here, with two illustrating how ISSRM and its Domain Model is used as a security risk management process and as a reference when applying concepts that enhance the security risk management process. The third work highlights the use of STRIDE in security risk management.

2.1.1 Analysis of Digital Security Threats in Aviation Sector

This is a research work by [38] illustrating the use of the ISSRM methodology and its Domain Model in the Aviation Sector specifically for the Airline Turnaround Process. This research was carried out as a continuation of another master thesis work - "Service Brokering Environment for an Airline" which demonstrated how an organization could transform its business processes to enable enterprise collaboration. The research work by [38] was done by following a scientific approach to ISSRM in solving the security issues in the Airline Turnaround process caused by collaboration between airlines and service providers in the aviation sector. The approach composed of three steps;

(i) identify assets that are involved in the collaboration,
(ii) determine the risks by exploring the risk components of the identified assets, and
(iii) apply security requirements and controls to mitigate the risks on these assets.

The research work also included an evaluation performed to establish how security requirements and controls reduced the risks, including a simulation to illustrate its validation process. By using an approach in line with the ISSRM methodology, the research work provided a way to counter threats relevant to the aviation sector showing evidence in simulations that illustrated a significant risk reduction.

2.1.2 Securing Airline Turnaround Processes using Security-Risk Oriented Patterns

Here, the ISSRM methodology was used as a foundational reference when combining specific concepts that aid enhancements in the aspect of security risk management in information systems. This research work [37] focused on the use of security risk-oriented patterns, developed using the ISSRM methodology domain model also for the purpose of securing the Airline Turnaround process. As software programs generally tend to run into similar problems, errors and attacks that may not require new solutions, a security pattern is useful in describing particular recurring security problem arising in a specific security context, and providing a generic scheme for a security solution.

Although there are numerous classification systems used to categorize security patterns for the purpose including resources for threat patterns such as CAPEC [4] and STRIDE [22], this research work focuses on the use of Security-Risk Oriented Patterns to find security risk occurrences in business processes and also present mitigations for these risks. It was proffered that by using this approach, business analysts will be provided with means to elicit and introduce security requirements to business processes whilst reducing the efforts needed for risk analysis and risk management.

2.1.3 Online Banking Security Analysis based on STRIDE Threat Model

This paper [40] carries out a system threat analysis method that combines the STRIDE threat model and threat tree analysis in such a way that improves the efficiency of threat analysis and also provides practicability. As there was a lack of systematic and holistic procedures in the use of threat tree for threat analysis, they apply the STRIDE threat model to the online banking system. This was done by carrying out an analysis of business assets, constructing a STRIDE threat model to identify threats and establishing a threat tree. It is proffered that applying this method to the online banking system threat analysis can provide guidance for system security analysis and evaluation.

From the research works discussed in sections 2.1.1, 2.1.2, and 2.1.3, it can be seen that;

- The ISSRM approach and its Domain model is a viable methodology that is used in security risk management. However, not enough work has been done on a method that focuses on threat analysis within the ISSRM methodology, allowing for a more consistent threat analysis to risk management procedure while following the guidelines of the ISSRM methodology and its Domain model.
- The STRIDE threat analysis is useful in providing a systematic procedure to threat analysis. However, a structured approach following from threat analysis to risk treatment in a security risk management process, following the ISSRM methodology, has not yet been carried out.

2.2 Model Representation for Security Risk Management

As system software development and maintenance for business continuity typically involve different stakeholders with different goals, needs, requirements and system expectations [27], addressing different viewpoints and coming to some agreement about them is a challenge. The use of various modeling techniques to illustrate these ideas in a consistent and coherent manner becomes helpful.

Business Process Model and Notation (BPMN) is a business-friendly language for constructing business process models. BPMN has been aligned with the ISSRM domain model as seen in research by [1] and thus, could be used for security risk management although the BPMN language was not explicitly dedicated to security modeling. Constructs of the language when oriented to security have been documented in research by [1] and [20].

Understanding the business process is the first step that allows the analysis of business needs (which security is a part of). With security considered, stakeholders can be aware of potential security threats, analyze risks and its impact and then design and implement appropriate countermeasures that will improve secure system development and functionality in the future. As such, models are a way to communicate the system to be built and so making a model of the system, aids discovery of threats without getting bogged down with too many details.

This security risk-oriented BPMN language is being used for this thesis research for the purpose of illustrating asset identification and elicitation, security requirements implementation and security countermeasures.

2.3 Threat-driven Perspective to Security Risk Management

Threat modelling in security risk management is more than one activity in the chain of discovering and mitigating security risk, as it begs the question of what is being built, what can go wrong when it is built, what should be done when things go wrong and if the analysis carried out is useful [33]. These threats are not to be discovered haphazardly, but in line with the vulnerability that it can exploit, depending on the system assets available, that serve to make sure that the business assets run as intended. The systematic discovery of threats in relation to the system domain, following a structured process to discovering the risks posed by these threats in order to develop security risk treatment procedures that aim to mitigate the risks whenever it arises is the purpose of this threat-driven perspective used in the research work.

Threat modelling, in some ways is like programming with no one ideal language for all tasks and so, there is no one way to handle threat modelling [33]. One method to threat modeling was introduced by [22] was STRIDE. In this research work, a STRIDE threat-based approach for security risk management considers the following as seen in Figure 3;

- The system being built, represented by its business process using the common BPMN notation language.
- What can go wrong, elicited using the STRIDE method;
- What should be done when things go wrong, as illustrated in the risk management procedures carried out based on the STRIDE threats and then risks elicited;
- The validation of the analysis by experts.

This approach is in line with the ISSRM procedure of first identifying the assets through *context and asset identification* to discovering the threats using a STRIDE based method which takes much into consideration, the *security objective determination* of the system, and proceeds to a structured elicitation of the impact of the threat and the resulting risk through *risk analysis and assessment*. The approach then moves forward to address the risk that has been elicited through *risk treatment* procedures, *security requirements definition* and considerations in the *selection of controls and implementation.* Being in line with ISSRM, the approach also follows the domain model in its structure.

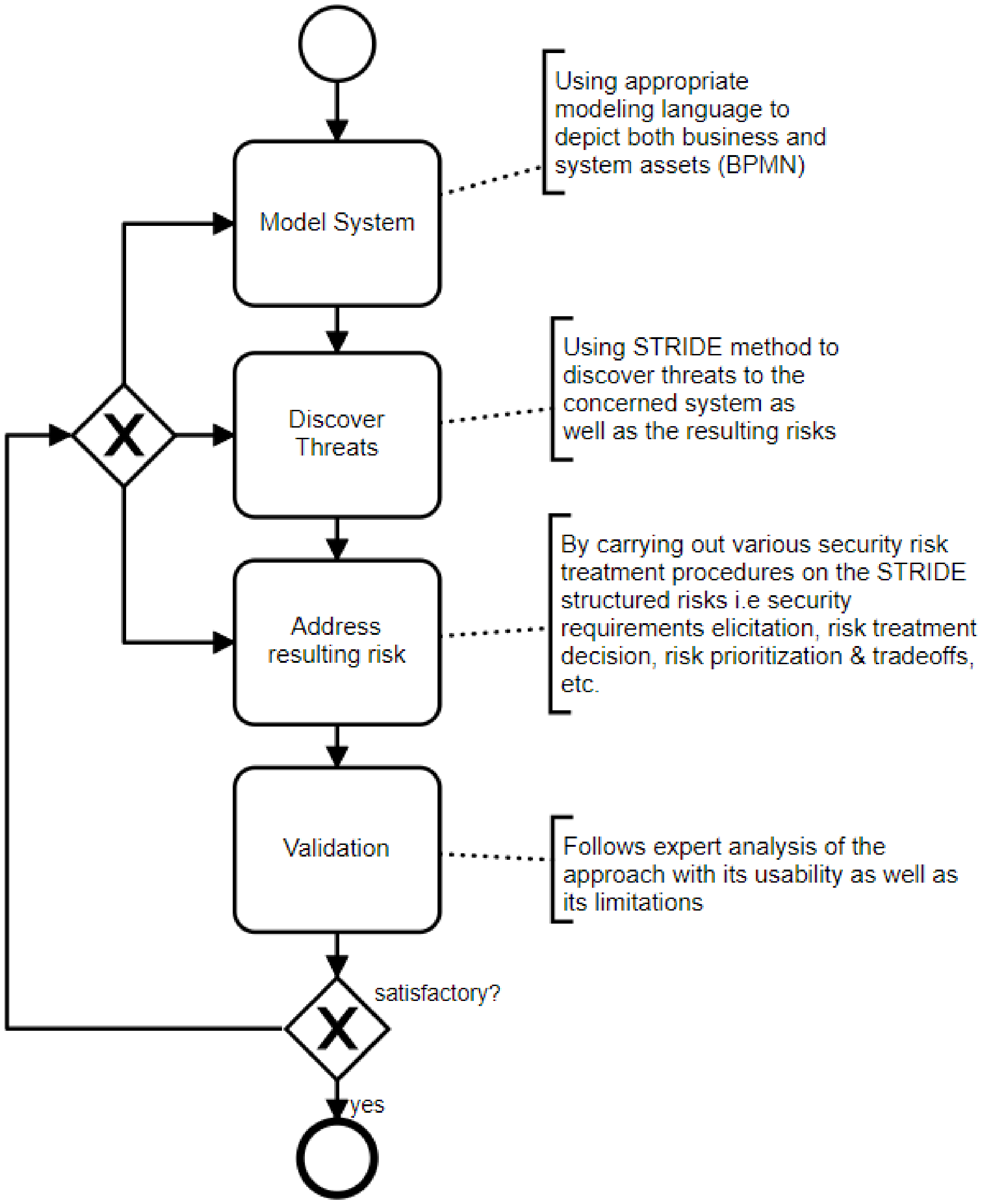

Model System
Using appropriate modeling language to depict both business and system assets (BPMN)
Discover Threats
Using STRIDE method to discover threats to the concerned system as well as the resulting risks
Address resulting risk
By carrying out various security risk treatment procedures on the STRIDE structured risks i.e security requirements elicitation, risk treatment decision, risk prioritization & tradeoffs, etc.
Validation
Follows expert analysis of the approach with its usability as well as its limitations
satisfactory?
yes

Figure 3: Threat-driven Approach

As this threat-driven approach to be used is based on STRIDE, there is need to elaborate on why STRIDE was chosen. STRIDE is a mnemonic that stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [36]:

- **Spoofing**: pretending to be something you are not or someone you are not [33]. Here, an attacker might pretend to be a legitimate customer accessing a Webshop, so there must be a way to authenticate Customers.
- **Tampering:** modifying something that you are not supposed to modify [33]. Here, an attacker might tamper with the data as it flows back and forth the Webshop server.
- **Repudiation**: claiming you didn't do something (regardless of if this is true or not) [33]. In this case, is there the presence of system logs, collated with the right information, protected against tampering?
- **Information Disclosure**: exposing information to those who are not authorized to view it [33]. In this case, what happens if a Customer is able to access information concerning other Customers in the Webshop?
- **Denial of Service**: attacks that are designed to prevent a system from providing its intended service by crashing it, slowing it down, or filling up its storage [33]. So, what could happen if a thousand customers connect simultaneously to the Webshop when there is news of huge discounts?
- **Elevation of Privilege**: when a program or user can to do things (technically) that they're not supposed to be able to do [33]. If the customer web front-end is the only way for a Customer to access the Webshop, are there controls to enforce that?

STRIDE helps to find, recognize and model these threats on a system. The application of STRIDE has been known to be easy to use, produce a significant number of threats for analysis and result in the relatively high number of correctly determined security threats [41].

There are other classifications of threats that have been identified such as one by Uzunov and Fernandez in [5]. This type of classification presents a security threat taxonomy for distributed systems by separating between *system threats* and the *threats to the security of the infrastructure of the system* thereby coming up with eight classes of system threats (identity attacks, network communication attacks, network protocol attacks, passing illegal data attacks, stored data attacks, remote information inference, loss of accountability, and uncontrolled operations) and four classes of threats to the security of the infrastructure of the system (cryptographic attacks, countermeasure attacks, configuration/administration attacks, and network protocol attacks) [20]. However, these methods have as a priority, the classification and categorization of threats, over its elicitation. Another method for threat modelling is the use of attack trees that provide a way of describing the security of systems based on various attacks that could possibly occur [32]. An attack tree relevant to the system being built is helpful in identifying threats; however with complex systems, using attack trees may become distracting or tedious. Also, attack trees lack some of the structure that STRIDE contains that is more beneficial for the risk management procedure.

So, for the purpose of this thesis research, STRIDE would be focused on. The selection of the STRIDE approach is because of its suitability to the concerned system and how easy it is to elicit threat scenarios. Also, each of the STRIDE scenarios is the opposite of security properties a system should have which are;

- **Spoofing** – *Authentication*
- **Tampering** – *Integrity*
- **Repudiation** – *Non-repudiation*
- **Information Disclosure** – *Confidentiality*
- **Denial of Service** – *Availability*
- **Elevation of privilege** – *Authorization*

This thus covers the security needs of any system with authentication, authorization and non-repudiation being secondary security properties. The connection of each STRIDE mnemonic to security property is also used for risk mitigation, as it guides the system stakeholders on how to mitigate the risks under each category by for example, implementing authentication mechanisms to treat spoofing risks. This reveals the scope covered by STRIDE and how useful it is in finding attacks in a system. The thesis research does not use STRIDE mainly as a categorization but also to elicit threats. Thus, carrying out threat elicitation into a structured approach to security risk management in the system is focused on.

One element not well covered in STRIDE is the identification of vulnerabilities and so for this, a taxonomy of vulnerabilities in software systems will be used as discussed in [35]. Also, in finding threats, STRIDE may be too high level and thus may not provide a detailed list of attack patterns to identify threats. These can be done using attack libraries such as CAPEC and OWASP Top Ten [27]. CAPEC [4] (MITRE's Common Attack Pattern Enumeration and Classification) has a highly structured set of about 476 attack patterns that have been organised into 15 groups is highly useful in this case. Also, the OWASP Top Ten list is a list with well-balanced attacks and backing information including threat agents, attack vectors, security weaknesses, technical and business impacts as well as vulnerability and mitigation details for the attack. Both the OWASP Top Ten and CAPEC serve as positive supplements to STRIDE. For security countermeasures, the security standard NIST SP 800-53[13] has within it, items that also aligns with one or more of elicited STRIDE threats.

2.4 Summary

This chapter discussed the risks in e-commerce systems as well as security risk management approaches available that target the risk management issue with security standards. The ISSRM approach and its domain model is provided as the preferred methodology for dealing with security risks in information systems. Previous work using the ISSRM methodology and STRIDE for security risk management activities were analysed to form the background of the thesis work. This opened a discussion on the threat-driven approach to security risk management in line with the ISSRM methodology and its domain model. STRIDE was introduced as the driver for threat modelling providing a consistent and structured risk management procedure in the midst of evolving threats. Also, security risk-oriented BPMN language introduced as being used to aid security risk illustrations.

3 Assets in E-commerce System

This Chapter seeks to answer the **RQ1** – *How can relevant assets for an e-commerce system be identified?* In order to answer this, the following questions are necessary;
RQ2.1: What can be used to identify and elicit assets in an e-commerce system?
RQ2.2: What are the assets that pose security concern in an e-commerce system?
RQ1.3: What is the importance of asset identification to risk management procedure?

By providing answers to these questions, the identification of relevant assets to an e-commerce system can be illustrated.

3.1 The E-commerce System and its Components

E-commerce refers to the transactions of buying or selling of products or services over the Internet and this is becoming popular because of its ease of use and convenience. Over the years, there has been a notable broadening of the online product types from books, computer software and hardware which had dominated e-commerce to including fashion (shoes, clothes, and jewelry.), household goods, toys and so on [24]. Today, many e-commerce websites may choose to specialize in some type or category of a product such as fashion, or sell a wide range of products as previously listed, such as which is seen in the popular e-commerce website, Amazon. A lot of popular e-commerce activities are directed at customers (Business to Consumer (B2C) type) as in the case of online retail stores and this e-commerce type will be focused on in this thesis because this deals with a lot of transactions that involve a significant portion of individuals, giving away sensitive information.

For the purpose of further analysis, defining what an e-commerce "*system*" refers to is imperative. In a practical setting, a system can be understood as a set of correlated phenomena, involving the following [20] with examples as refers to a B2C e-commerce system;

i. a product, service or a component (e.g., clothing, electronics, food order service or car rental service),
ii. the infrastructure needed to combine the products or components (e.g., Webshop website and warehouse),
iii. the applications that are used to support activities (e.g., customer browser, Webshop server, Webshop payment system, and Webshop inventory system),
iv. information technology staff who support the above-mentioned components (e.g., Webshop server administrator)
v. internal employees, management, and third-party entities, who use the technology to achieve the business goal (e.g., Webshop Customer Support, Webshop Merchant, Shipping company, and Payment Service Providers)
vi. Webshop customers and other external users, who buy products and use services of the system.

From the above explanation, an e-commerce system can be seen as much more than a website, a customer and a merchant. Security asset-related concepts in an e-commerce system will follow an understanding of the e-commerce system, its security objectives, and its processes to then enumerate its security assets (business and system assets).

3.2 Security Objectives in an E-commerce System

When security risks are considered, this implies the acceptance of a security need in the system. The security objective is a property that describes the security need of a system, typically expressed through the security objectives which are security characteristics of business assets. An e-commerce system, like any information system has the following security objectives;

Confidentiality: this describes the state in which data is protected from disclosure to parties that are unauthorised to view it. For example, loss of confidentiality occurs when a Customer username and password is disclosed to parties other than the Customer.

Integrity: this describes the state in which data is not altered or modified either due to malicious intent (intentional sabotage of Webshop Storage) or accidentally.

Availability: this describes the fact that authorised persons can access business assets within the appropriate period of time. For example, a Webshop product list must be made available 24/7 to Customers.

A security objective is a property of the business assets and it is possible that a security criterion can be a constraint of several different business assets, or not constraint any of them as one or several security criteria can be needed to assess the significance of risk. However, if a security criterion concerned by none of the risks, in that case, there is no relevant impact for this criterion. There are other security criteria which may be added when the context requires and are deemed secondary. They are;

Non-repudiation: this is a form of accountability and assurance on the business asset describing the proof of the integrity of the concerned business asset.

Authorisation: describes permissions on the business asset for the purpose of creation, modification, retrieval and deletion. For example, checkout service can only be carried out by a legitimate Customer of the Webshop.

Authentication: describes a verification of the identity of the supplied business asset, which if successful grants a defined level of access.

These primary and secondary security criterions are the basis for the STRIDE threat modelling approach.

3.3 The E-commerce Order Fulfilment Business Process

Knowing the business process is a significant aspect of managing security risks in any system. The business process illustrates the context of the organization, the assets involved and its activities as seen and understood by a business analyst [3]. It is possible to extract the business process by following the logical flow of how the application should work in order to fulfill its purpose. This was discovered through a study of popular e-commerce retail websites to discover a general application workflow to achieving its purpose which is in this scope – order fulfillment. The major processes discovered are highlighted in Figure 4 [14];

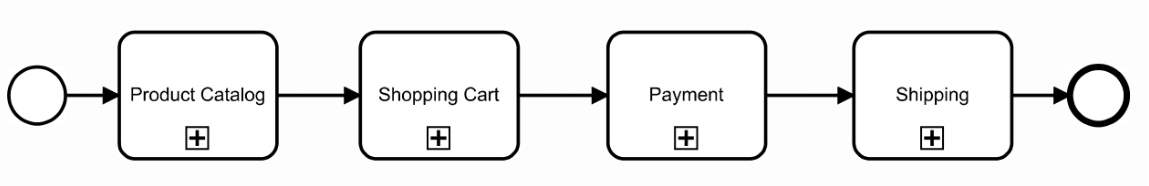


Figure 4: Value Chain

In Figure 4, the value chain consists of the main value – an *order*, which is created as a result of the process steps. The process begins with viewing the *product*, provided by the *Product Catalog process*. After a product is selected, it is added to the *Shopping Cart* where it is prepared for checkout. The *Payment process* allows for the *selected product* to be purchased and then the *Shipping process* takes the product to the Customer which completes the *order*. These processes are collectively shown in Figure 9.

3.3.1 Product Catalog

The product catalog or product list as seen in Figure 5, details product information needed to present any product to the customer and complete the transaction. Any company that seeks to sell products via e-commerce will contain this process. This product information consist of the product price, product description, product image, product identification number, product choices, options (color, size, and weight) and availability of the product [14]. This process must ensure the provision of correct information about the product.

3.3.2 Shopping Cart

Online shopping carts are much equivalent to the real-world shopping carts; both allow shoppers to set aside selected purchases in preparation for checkout. The shopping cart process, illustrated in Figure 6, allows customers to select a product, review selected products, edit selections as necessary, remove selection, and then actually make the purchase by clicking checkout button [14]. Finally, the checkout procedure allows the customer select products from the shopping cart that the customer intends to buy at the moment. This could be all the products available in the cart and also partial products in the cart. This process also prepares the necessary information needed to the next process which is the payment process. Information concerning the shopping cart process is automatically stored in the database.

3.3.3 Payment Process

The shopping cart process, typically works in conjunction with the payment process illustrated in [14]. During payment, a customer provides his/her payment card details after being directed to the payment gateway and this information is sent to the bank. The bank checks the customer's account and can either authorize the payment or not. This operation, if approved, allows the bank to send approval notification to the customer and perform the order transaction and transfer payment to the merchant account. If this operation is denied, the customer is notified that the transaction cannot be completed. After a successful payment process, information is sent to the merchant to start the shipping process.

Usually, to make purchases on the e-commerce platform through checkout, a user should already be registered and logged in to the site. This is true of many popular e-commerce sites such as Amazon and eBay. The data provided during registration will include information needed for identifying the user during account login and for shipping, billing and fraud-mitigation purposes.

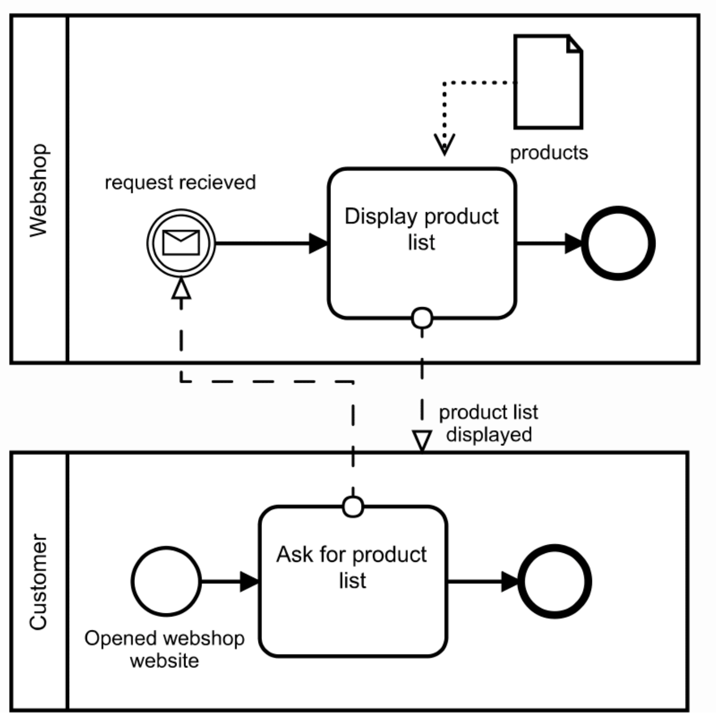


Figure 5: Product Catalog Process

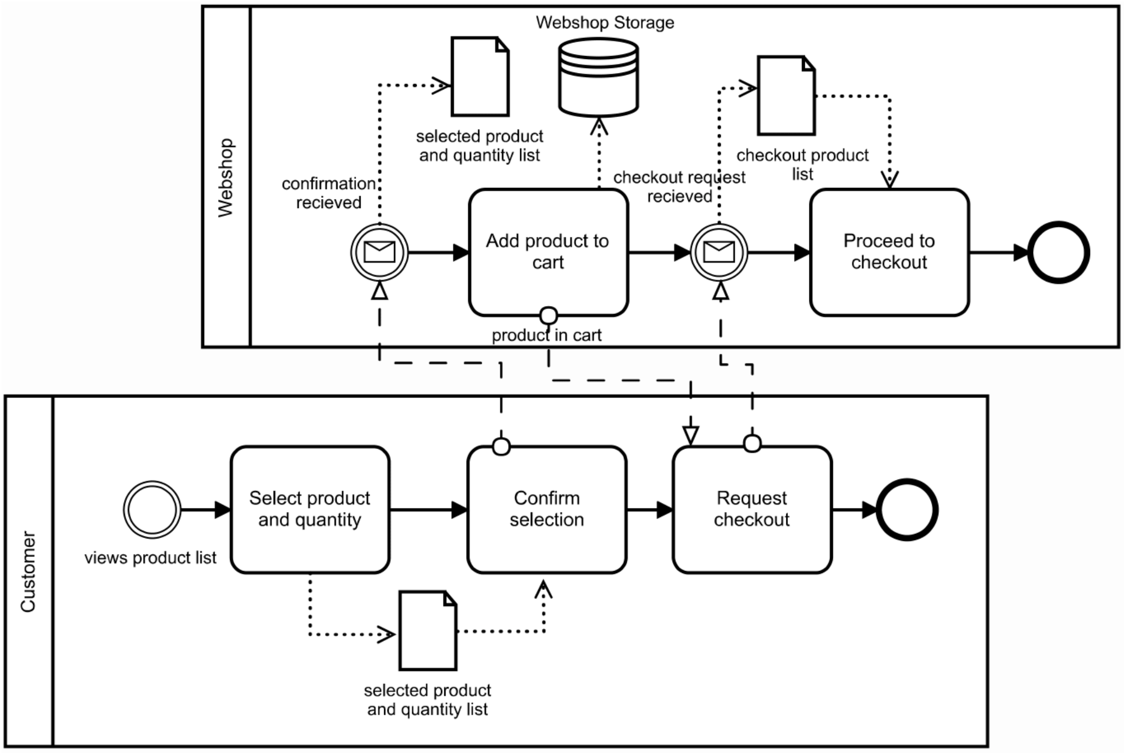


Figure 6: Shopping Cart Process

Some e-commerce sites have decided to provide a way to skip this procedure if the customer does not wish to complete registration. This is done for a number of reasons such as the reduction of shopping cart abandonment, allowing the customer to carry out transactions as guest. If this procedure is applied to a Webshop, it benefits the security objective of confidentiality as the Webshop will not store the provided personal information thereby reducing the impact of attacks that seek to collect sensitive information from the Webshop.

Both procedures have its pros and cons, but for the purpose of this research work, the focus is on Webshops that use only registration procedure.

3.3.4 Shipping

This process as illustrated in Figure 8, allows the customer's purchased product to be sent out to the customer using a defined shipping method. The choice of shipping method can be defined at the point of checkout or may be one predefined by the Merchant. The shipping process is reached after notification of purchase and payment information has been received by the merchant. The merchant makes the purchased product ready for shipping and sends it out to the defined user shipping address. From the information provided, a merchant can now [28];

1. Determine which products to package and the total size and weight and makes it ready for shipping.
2. Confirm the shipping destination from customer-provided data.
3. Determine the shipping carrier to be used, sometimes selected by the customer or enforced by the merchant. The shipping cost is usually paid during checkout.
4. Send the product out via the shipping carrier to the customer.

Also, this process also involves user confirmation of having received the product, customer rating of product and in some situations, returns and refund process.

3.4 Security Assets in an E-commerce System

In section 3.1 the e-commerce system was defined, showing its major components and in section 3.2, the functionality of e-commerce business process was discussed, demonstrating the assets involved which will aid modelling in a way that is easier to understand by business analysts. On the other hand, the system assets of an e-commerce system can be seen in material and tangible elements of an e-commerce system components as well as the business processes explained in section 3.3. Human beings that deal with e-commerce processes can also be classified as system assets [20] which include Customers, internal employees of the e-commerce system (e.g., Webshop Merchant). For each business process function (business asset) there are two or more system assets that support these functions. These system assets are also characterized by the vulnerabilities which are exploited in the event of a threat and results in security risks. For example, a Merchant can be vulnerable to social engineering threat and an Input interface can be vulnerable to SQL Injection – an input validation threat.

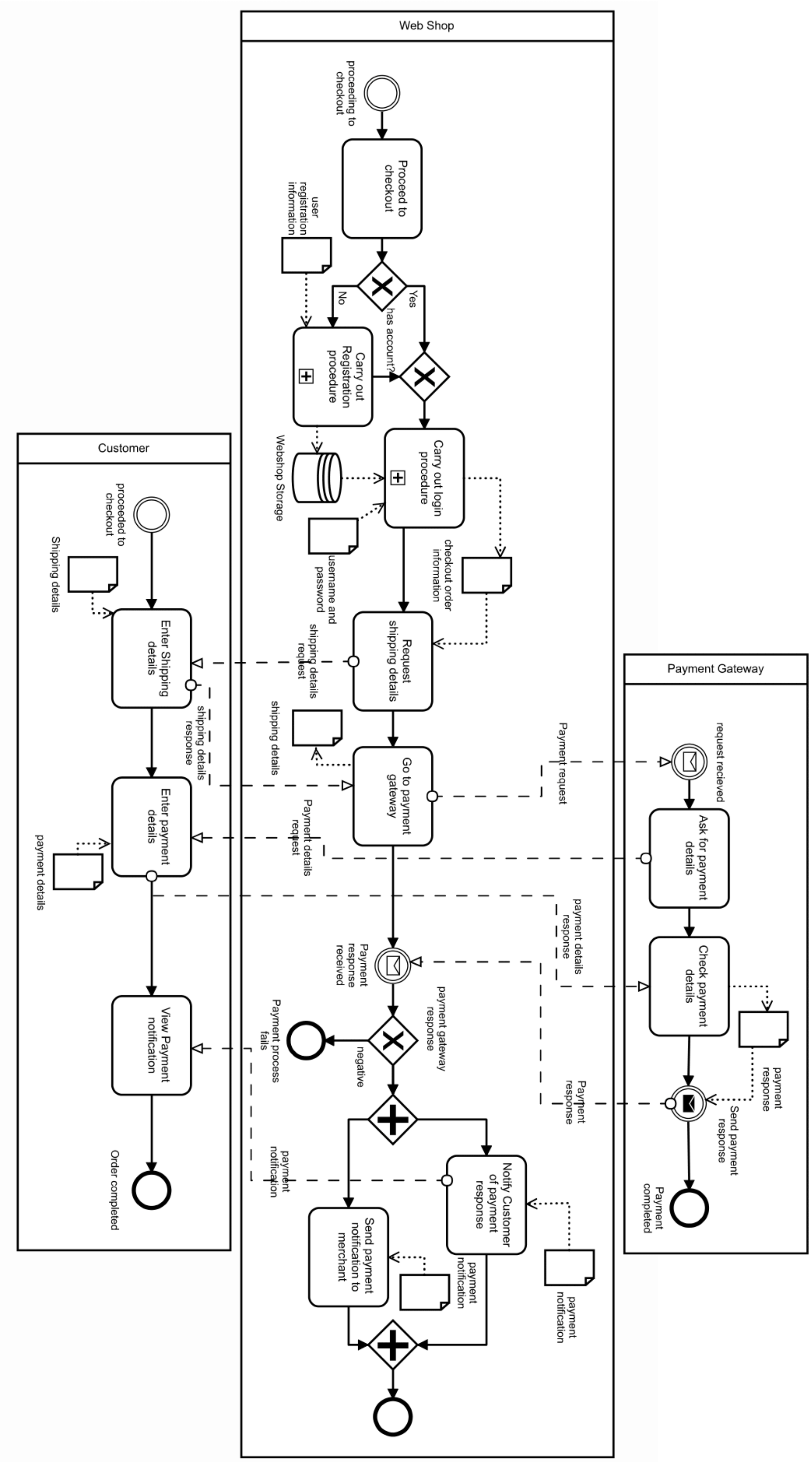


Figure 7: Payment Process

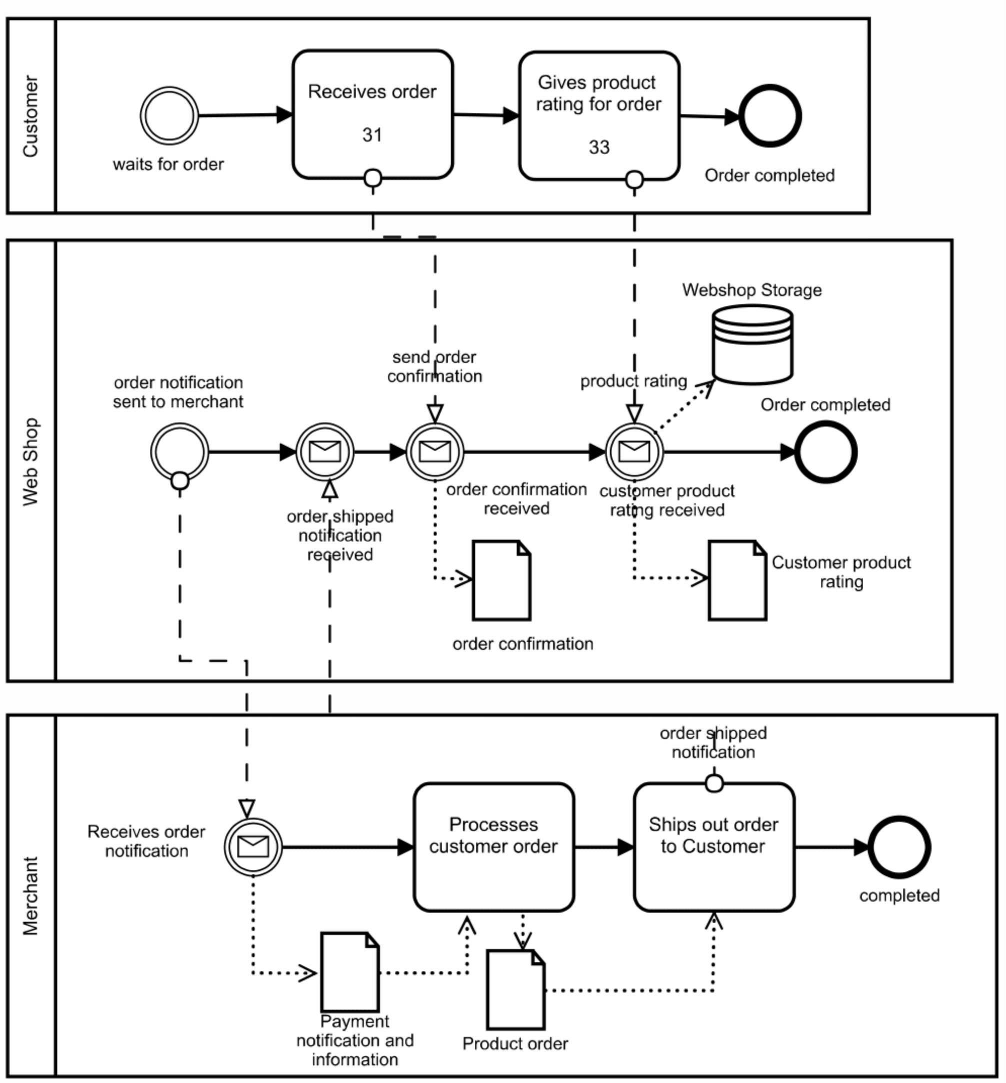

Customer
waits for order
Receives order
31
Gives product rating for order
33
Order completed
Web Shop
Webshop Storage
send order confirmation
product rating
order notification sent to merchant
Order completed
order confirmation received
customer product rating received
order shipped notification received
Customer product rating
order confirmation
Merchant
order shipped notification
Receives order notification
Processes customer order
Ships out order to Customer
completed
Payment notification and information
Product order

Figure 8: Shipping Process

Business assets for the scope of this research work can be derived from the business process. The use case below describes the business process of the Webshop in the following steps, of which the *Webshop order fulfilment process* itself can be considered a business asset;

1. The Webshop Customer opens the Webshop website.
2. The Customer requests for the *product list.*
3. The Webshop receives the *product list request.*
4. The Webshop *displays the product list*.
5. The Customer *selects product and quantity*.
6. The Customer sends *product selection confirmation.*
7. The Webshop receives *product selection confirmation*.
8. The Webshop adds *selected product and quantity list* to cart
9. The Customer *requests checkout*.
10. The Webshop receives customer *checkout request.*
11. The Webshop *proceeds to checkout*.
12. The Webshop checks if the customer *has account*?
13. If the customer does not have an account with the Webshop, the Webshop will *carry out registration procedure*.

14. If the customer has an account with the Webshop, the Webshop skips registration procedure.
15. The Webshop will *carry out login procedure*.
16. The Webshop *requests shipping details.*
17. The Customer *enters shipping details.*
18. The Webshop will *go to payment gateway*.
19. The Payment gateway *asks for payment details*.
20. The Customer *enters payment details.*
21. The Payment gateway *checks payment details* received from the customer.
22. The Payment gateway *sends payment response* to the Webshop
23. The Web Shop *receives payment response* from the payment gateway
24. The Webshop checks *payment gateway response*.
25. If the response is negative, *payment process fails*.
26. If response is positive, the Webshop will *notify Customer of payment response* and payment *send payment notification to merchant*.
27. The Customer *views payment response.*
28. The Merchant *receives payment notifications and payment*.
29. The Merchant will *process customer order*.
30. The Merchant *ships out order to Customer* and sends *order shipped notification* to the Webshop.
31. The Customer receives the *order*.
32. The Customer *sends order confirmation* to the Web Shop.
33. The Customer *gives product rating for order.*
34. The Webshop receives *customer product rating* for order.
35. Order completed.

From this use case, it is possible to elicit the system assets that support business assets. The following system assets will support business assets further down in the research work.

1. Product: Webshop
2. Infrastructure: Webshop Website
3. Applications/components used to support activities: Webshop Server, Webshop Storage, Webshop API, and Webshop Login Interface.
4. IT Staff: Webshop Admin
5. Customers: Webshop Customer

The *Webshop* is the name given to the e-commerce application in this case. It provides a graphical user interface seen as the *Webshop Website* and displays, collects and manipulates input provided from the *Webshop Customer,* and the *Webshop Admin.* The *Webshop* application consists of a *Webshop Server* that processes requests sent to the *Webshop* from external systems such as login requests or checkout requests. For the collection of input particularly for login purposes, the *Webshop* uses its input interface – the *Webshop Login Interface*. The Webshop is administered using the *Webshop Admin Interface.* Other system assets used by the concerned *Webshop* includes *Webshop API* used for development purposes for the *Webshop* and the *Webshop Storage* for storing business sensitive data.

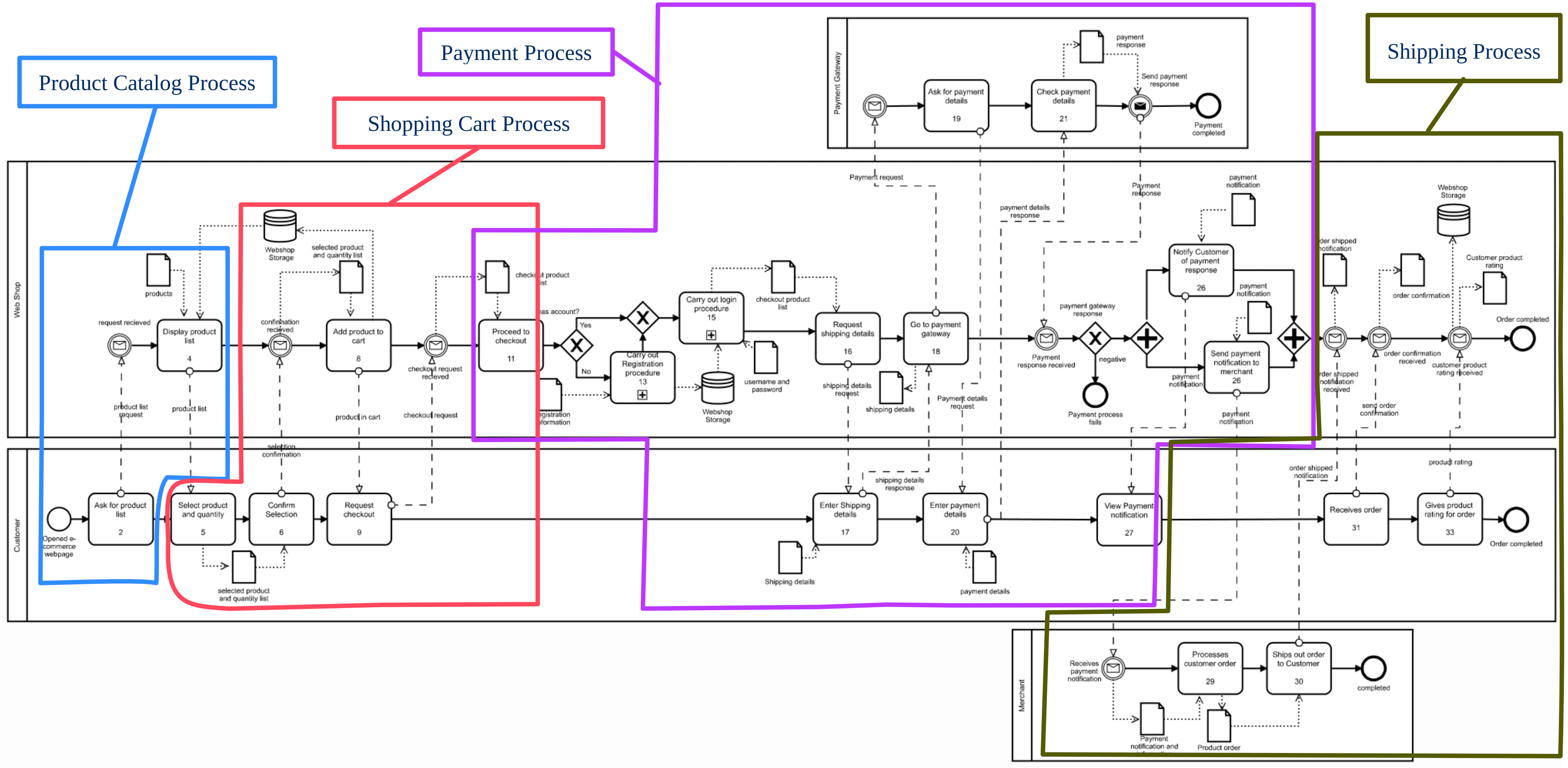


Figure 9: E-commerce Webshop Business Process

(This is the structured perspective of the model, low fonts of labels are left intentionally)

3.5 Summary

In this chapter, the security assets in an e-commerce system and the methods of identifying these assets were discussed. These assets were identified through a study done to develop a business process illustrating the business specific assets as well as their supporting business assets. As an e-commerce system Webshop contains many complex processes, one process – the order fulfilment process, was considered and the security assets elicited accordingly. Security objectives, a security characteristic of the business assets of a system, were also discussed, introducing these criterions as the basis for the STRIDE modelling approach.

4 Security Risk in E-commerce Systems

This chapter provides answers to the **RQ2** – *What are the security threats as well as its resulting risk to an e-commerce system?* In order to answer this, the following questions are necessary;
RQ2.1: What are the vulnerabilities of assets in an e-commerce system?
RQ2.2: What method can be used to identify security threats to an e-commerce system?
RQ2.3: What are the impacts of security threats that result in risks in an e-commerce system?

With these questions answered, information about vulnerabilities of the system assets discovered in Chapter 3, e-commerce threats, impacts and the resulting risk scenario can be illustrated.

4.1 E-commerce Risk Landscape

E-commerce is a profitable target. For example, large payment processing firms, have a significant risk of fraud (being up to 0.9 %) and even though e-commerce fraud rates have become stabilized in recent years—due, in part, to retailers' increased vigilance—in 2009 merchants still lost about $3.3 billion to online fraud [34].

The e-commerce industry suffered, losing customer trust and customer base, with various payment gateways and bank authorization processes vulnerable to attacks such as man-in-middle attacks. A simple denial of service (DoS) attack could result in online stores or portals being inaccessible and undoubtedly interrupts the online business activities. The most serious of these scenarios are those that involve the theft or destruction of customer's sensitive information. Others could be website spoofing, payment card information theft, malware attack (using Trojans, viruses, worms, and bots), hacker infiltration, vandalism, and identity theft. These attacks leave lasting effects on the targeted e-commerce platform. Attacks against Top B2C e-commerce establishments especially online retail stores have consistently remained at breach levels of severe (7 – 8.9) to catastrophic (9 – 10) as seen in Table 1 [58] with breaches involving personally identifiable information of customers, transactional data, and credit card information.

Relevant risks in information systems, given its prevalence and the business's dependence on it, should be analyzed. The development and use of security risk scenarios is a core approach to bring realism, insight, some organizational engagement, improved analysis and structure to the complex matter of security risk [25]. A security risk scenario can be seen as a security event that can lead to a business impact, when and if it should occur. Thus, for security risk scenarios to be complete and usable for assessment, they should contain the following components, illustrated in the domain model;

- Vulnerability of system asset
- Threat agent
- Attack method
- Resulting threat
- Threat Impact

Table 1: Top Retail Data Breaches in Retail [3]

Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Risk Score
Target	110,000,000	11/04/13	Financial Access	Malicious Outsider	United States	10.0
Home Depot	109,000,000	09/02/14	Financial Access	Malicious Outsider	United States	10.0
eBay	145,000,000	05/21/14	Identity Theft	Malicious Outsider	United States	10.0
Homeplus Co./Tesco PLC	24,000,000	07/07/14	Identity Theft	Malicious Insider	South Korea	9.5
AliExpress	300,000,000	12/08/14	Account Access	Accidental Loss	China	9.5
VTech Holdings	11,686,131	11/14/15	Identity Theft	Malicious Outsider	Global	9.0
TalkTalk	4,000,000	10/22/15	Identity Theft	State Sponsored	United Kingdom	8.9
Gaana.com, Times Internet	10,000,000	05/28/15	Identity Theft	Malicious Outsider	Pakistan	8.9
Rakuten and LINE Corp	7,850,000	04/17/15	Account Access	Malicious Outsider	Japan	8.8

The ISSRM domain model will now be applied to identify security risk scenarios in the *order fulfilment process* which encompasses the *Product catalog process*, *Shopping cart process*, *Payment process* and *Shipping* process. This activity starts with the identification of vulnerabilities (a characteristic of the system assets), the likelihood of threats to exploit the listed vulnerability, impact of the threat event, describing how the security event will harm the assets (business assets and system asset) and how it negates the security criteria and finally, the security risk.

The domain model shows that security risks arise as a result of the combination of a threat with one or more system vulnerabilities which leads to a negative impact that harms at least two or more assets [20].

4.2 Vulnerabilities in E-commerce Systems

E-commerce systems, like any other electronic-based system, has within itself various vulnerabilities, susceptible to exploitation leading to threats that causes security risks. E-commerce system vulnerabilities are inherently the characteristics of the identified system assets of the system that can be exploited leading to a security risk. In [20], it is advised that using existing knowledge (e.g., vulnerability catalogues) and (previous) expertise will be helpful in characterising potential vulnerabilities of considered system assets. There are some vulnerability catalogues/databases including the National Vulnerability Database (NVD) [25], CWE [5], the US-CERT Vulnerability Notes Database [39], OWASP top 10 web application vulnerabilities [27] that one could use when developing and protecting software systems.

In an article by [41], the vulnerability of a system was revealed to exist at specific entry points within the system. Some entry points which an attacker can target in an e-commerce system are through the customer, the login interface between the customer and the e-commerce website server, the network connection between customer and e-commerce web server or the e-commerce web server. According to [30], finding vulnerabilities depend on the nature of the IT system and the stage of the system development. This could be;

- The design stage, where vulnerability identification should be focused on the security policies made, the planned security procedures, the system requirements and so on.
- The implementation stage, where identifying vulnerabilities should be focused on specific concerns such as the features of the system as described documentations, results of system testing, evaluations of such implementations and so on.
- The operational stage, where identifying vulnerabilities should include an analysis of the specific features of the security system in place, technical and operational measures that have already been put in place to protect the system, usage or management of the system by personnel, and so on.

With knowledge of the nature of the system, identification of vulnerabilities is rather easy as the scope is narrowed.

In [20], the vulnerabilities were discussed instead as software flaws or system errors that result in a security flaw and thus, security risk. The "Seven Pernicious Kingdom" taxonomy discussed in [20] concerning software vulnerabilities was suggested, giving classifications of common vulnerabilities in software systems. This classification included [35],

a. Input validation and representation: This includes vulnerabilities that are specific to input and output interfaces on the e-commerce system.
b. Application programming interface (API) abuse: This includes vulnerabilities specific to APIs which are probably under-protected. API abuse categories are common.
c. Security features: Software security does not mean security software. Chunking together security features on topics like authentication, cryptography, and privilege management, does not ensure security unless it is done right as it may lead to weak encryption mechanisms or insufficient Transport Layer Protection.
d. Time and state: These are defects related to unexpected interactions between threads, processes, time, and information within a system.
e. Error handling: This includes vulnerabilities that arise from the manner in which errors are handled within the system and how it is displayed.
f. Code quality: This includes vulnerabilities that arise from poor code quality leading to unpredictable behavior and poor usability.

g. Encapsulation errors: This includes vulnerabilities that arise from the inability to draw strong boundaries around sensitive parts of the application and setting up barriers between them. On a Web server, it might mean differentiating between valid authenticated data and data that should not be made available to that authenticated session.
h. Environment: As applications run on physical machines or are run by people or external processes, the interactions of the application with its environments such as Human (system administrator, system users), Physical environment or Third Party associations should be considered.

The taxonomy above is used to classify vulnerabilities in e-commerce systems as shown in Table 2. Vulnerabilities listed are classified according to the taxonomy discussed above.

Table 2: Taxonomy of Vulnerabilities

Taxonomy	Affected System Asset	Vulnerability Examples
Input validation and representation	Webshop Login Interface Webshop Server	**V1**: Lack of Input Validation of Webshop Login Interface
Application programming interface (API) abuse	Webshop API	**V2:** Insecurely protected Webshop API
Security features	Webshop server	**V3:** Improper Output Neutralization for Webshop server logs **V4:** Weak username and password combination
Time and state	Webshop server	**V5**: Origin Validation Error of Webshop Server.
Error handling	Webshop server	**V6**: Improper error handling of the Webshop server
Code quality	Webshop server	**V7**: Allocation of Resources Without Limits or Throttling in Webshop Server
Encapsulation errors	Webshop server	**V8:** Improper Authorization in Webshop
Environment	Webshop Admin	**V9**: Use of Insufficiently Random Values for sessionID Webshop Server

4.3 Security Threats in E-commerce Systems: STRIDE

Risks scenarios are developed from the existence of threat events having an impact on the concerned system. According to [41], in order to discuss threats in e-commerce, provided a model to analyze threat classification. Here threats were classified from two points of view: threat agents and threat techniques. In [20], a security threat is an event that is initiated by a threat agent using an attack method against one or more system assets by exploiting their vulnerabilities. Current attacks on e-commerce systems such as Webshops are similar to typical web applications. By exploring the attacker's perspective, the nature and existence of risks in the system can be analyzed. Also, proper defenses can only be established if the attack pattern or method can be predicted. The CAPEC's list of attack patterns [4] is a useful collection of specific attack patterns that result in threats relevant to the Webshop example and also to e-commerce systems. Out of the total attack patterns listed, nine relevant to e-commerce systems were collated and categorized. These attack patterns also contain estimations on attack severity, the likelihood of exploitation, technical impact as a result of attack motivation-consequences and mitigation, helpful when carrying out risk measurement activities.

The STRIDE threat modeling, introduced by [33] which helps to find, recognize and model these threats on a system has been known to be easy to use, produce a significant number of threats for analysis and result in the relatively high number of the correctly determined security threats [20] and will be applied in this research to derive security threats in e-commerce systems. It is the responsibility of those performing threat modeling and analysis to discover and describe the threats and attack vectors, within the unique context of a system under analysis. Table 3 illustrates a list of threats according to the STRIDE approach. Each of these threat scenarios is labelled according to their threat type.

4.4 Security Impact of Threats on E-commerce Systems

The combination of threat and the vulnerabilities of the system assets help to represent the event of the risk and the consequence of the risk known as impact. The impact essentially means that a threat agent was able to use the attack method and exploit system vulnerabilities and is typically seen as some appearance of strange files or programs, automatic sending of emails or messages, and system misbehaviour. These actions negate the confidentiality, availability and/or integrity of the business assets [20]. In order to define the impact of a threat on the system assets, the following can be specified;

(i) How security criteria are negated by the threat: This could result in the loss of confidentiality, loss of availability or loss of integrity of assets which can be represented on a discrete scale (e.g., low medium, high)

(ii) The harm to the business assets which could result to considerable financial losses, and loss in customer trust and confidence. This could be represented in continuous (e.g., monetary units) or discrete (e.g., high, medium, low) scales.

(iii) The harm to the system assets reflects the state of the system asset after its vulnerabilities have been exploited which includes bugs and malware infection. This could be represented same way as the harm to business assets.

However, for the risk examples in Table 4, the direct negation of security criterion as an impact of the threat event is considered, and metrics discussed further in Chapter 6.

As can be seen in Table 4, the security risks are derived from the combination of the threat event and impact of the threat. Each risk scenario is labelled according to its STRIDE category.

Table 3: STRIDE Approach for E-commerce System Threats

Threat type	Threat Event example	E-commerce scenario
S **(Spoofing Identity)**	**ST1**: An attacker with knowledge of Webshop sets up an Ad on social media with a malicious CSRF script that creates bad ratings on product orders using the victim's account	**V5:** Origin Validation Error of Webshop Server **Threat Agent** - An attacker with knowledge of Webshop sets up a malicious CSRF infected Ad on social media that creates bad product ratings on using the victim's account when clicked. **Attack method** - 1. Have knowledge of Webshop. 2. Set up a malicious Ad on social media with a malicious CSRF script that creates bad product rating on a Webshop product. 3. Customer clicks on the malicious link. 4. Bad product ratings are created using victim Customer's account if the customer is already logged in.
	ST2: An attacker compares valid sessionIDs provided by Webshop and brute forces to access a valid Customer session	**V9:** Use of Insufficiently Random Values for sessionID Webshop Server **Threat Agent** - An attacker with the means to compare valid sessionIDs and brute forcing to access a valid Customer session. **Attack Method** – 1. Login to Webshop with multiple accounts. 2. Observe session IDs issued by Webshop server. 3. Brute force valid session ID and replay generated sessionID. 4. Customer session is accessed.
T **(Tampering Data)**	**TT1**: An attacker tampers with the product price by exploiting the insecurely protected Webshop API	**V2**: Insecurely protected Webshop API **Threat Agent** - An attacker with the means to tamper with the product price by injecting malware into the insecurely unpublished protected Webshop API. **Attack method** - 1. Scan Webshop server to identify poorly hidden Webshop API 2. Bypass authentication in Webshop API and find the exposed interfaces by sniffing to expose interfaces that are not explicitly listed. 3. Discover unpublished functions 4. Craft and send malicious calls to include malware that controls product price on the Webshop.
R **(Repudiation)**	**RT1**: An attacker with the means to add entries to Webshop server logs to obfuscate illegal transactions on Webshop by exploiting the Improper Output Neutralization to Webshop server logs	**V3:** Improper Output Neutralization for Webshop server logs. **Threat Agent** – An attacker with the means to add entries to Webshop server logs. **Attack Method** – 1. Determine Webshop Server log file format by checking error messages. 2. Write a malicious script to provide feedback on log injection possibility. 3. Launch various logged actions with malicious data to determine what sort of log injection is possible. 4. Insert script to insert false entries into the log file alongside appropriate logging input when possible log injection is found.

I **(Information Disclosure)**	**IT1**: An attacker with the means to extract sensitive customer information from Webshop storage by sending crafted SQL injection statements through Webshop login interface.	**V1** – Lack of input validation of Webshop Login interface **Threat Agent** – An attacker with the means to extract sensitive customer information from Webshop storage by sending crafted SQL injection statements through Webshop Login interface. **Attack method** - 1. Go to Webshop. 2. Identify the vulnerable Webshop Login interface. 3. Repeatedly send crafted SQL injection statements through Webshop login interface. 4. Observe error message containing customer information from Webshop Storage to an unauthenticated malicious user.
	IT2: An attacker with the means to query Webshop web server for common directory names to access directory containing Customer transaction information in Webshop Storage.	**V8 –** Improper Authorization in Webshop. **Threat Agent** - An attacker with the means to access directory containing Customer purchase information in Webshop Storage. **Attack Method:** 1. Login to Webshop. 2. Send requests to the web server for common directory names. 3. Sequentially request a list of common base files to each directory discovered. 4. Access sensitive customer transaction information.
D **(Denial of Service)**	**DT1**: An attacker with the means to cause an error state in the Webshop server	**V6**: Improper error handling of the Webshop server **Threat Agent** - An attacker with the means to cause an error state in the Webshop server. **Attack Method** – 1. Explore Webshop server info and identify the vulnerable component. 2. Craft/search exploit for component and inject an exploit into Webshop server. 3. Cause server error state by exploiting inadequate error handling vulnerability in Webshop server. 4. Webshop unable to complete checkout requests.
	DT2: An attacker with the means to exhaust Webshop checkout service	**V7:** Allocation of Resources Without Limits or Throttling in Webshop Server **Threat Agent** - An attacker with the means to flood the Webshop server with multiple checkout requests and compromise the availability of Webshop checkout service. **Attack Method** – 1. Explore Webshop checkout process. 2. Craft malicious script able to generate more requests than Webshop server can handle. 3. Use this malicious script on Webshop. 4. Cause exhaustion of resources to perform Webshop checkout service.
E **(Elevation of Privilege)**	**ET1**: An attacker with knowledge of admin interface address and a list of common username and password combinations gains admin access to Webshop.	**V4:** Weak username and password combination **Threat Agent** - An attacker with the means to gain admin access to Webshop. **Attack method** - 1. Access JavaScript files for admin interface of the Webshop in a browser. 2. Go to admin login interface and try common usernames and password combinations. 3. Access to admin interface successful 4. Collect customer username and passwords from Webshop Storage. 5. Privilege escalation successful.

Table 4: STRIDE-based Security Risk Impact Analysis

Threat type	Security Risk	Impact analysis
S (Spoofing Identity)	**SR1**: An attacker with knowledge of Webshop sets up an Ad on social media with a malicious CSRF script that creates bad reviews on using the victim's account by exploiting the Webserver's inability to verify the origin of requests leading to the loss of Integrity of Customer feedback ratings.	**Impact**: Loss of Integrity of Customer feedback rating. **ST1**: An attacker with knowledge of Webshop sets up an Ad on social media with a malicious CSRF script that creates bad ratings on using the victim's account. **V5:** Origin Validation Error of Webshop Server
	SR2: An attacker with the means to compare valid sessionIDs and brute forcing to access a valid Customer session by exploiting the weak sessionID generated by Webshop Server leading to loss of confidentiality of Customer session.	**Impact**: Loss of Confidentiality of Customer session. **ST2:** An attacker compares valid sessionIDs provided by Webshop and brute forces to access a valid Customer session **V6** – Weak sessionID generation of Webshop Server.
T (Tampering Data)	**TR1:** An attacker tampers with the product price by exploiting the insecurely protected unpublished Webshop API leading to the loss of Integrity of Product prices.	**Impact:** Loss of Integrity of Product prices. **TT1:** An attacker tampers with the product price by exploiting the insecurely protected Webshop API **V2** – Insecurely protected Webshop API
R (Repudiation)	**RR1**: An attacker with the means to add entries to Webshop server logs to obfuscate illegal transactions on Webshop by exploiting the Improper Output Neutralization to Webshop server logs leading to loss of integrity of Webshop process.	**Impact**: Loss of Integrity of Webshop server logs **RT1:** An attacker with the means to add entries to Webshop server logs to obfuscate illegal transactions on Webshop by exploiting the Improper Output Neutralization to Webshop server logs **V3:** Improper Output Neutralization for Webshop server logs.
I (Information Disclosure)	**IR1**: An attacker with the means to extract Customer information from Webshop storage by sending crafted SQL injection statements through Webshop Login interface by exploiting the lack of input validation of Webshop login interface leading to loss of confidentiality of Customer information.	**Impact**: Loss of Confidentiality of Customer information. **IT1:** An attacker with the means to extract sensitive customer information from Webshop storage by sending crafted SQL injection statements through Webshop login interface. **V1**: Lack of Input Validation in Webshop Login Interface
	IR2: An attacker with the means to query Webshop web server for common directory names to access directory containing Customer transaction information in Webshop Storage by exploiting the improper authorization in Webshop leading to the loss of confidentiality of customer transaction information.	**Impact**: Loss of Confidentiality of Customer transaction information. **IT2:** An attacker with the means to query Webshop web server for common directory names to access directory containing Customer transaction information in Webshop Storage. **V8 –** Improper Authorization in Webshop.

D **(Denial of Service)**	**DR1**: An attacker with the means to cause an error state in the Webshop server and Webshop website crashes by exploiting the improper error handling of the Webshop server leading to loss of availability of Webshop website service.	**Impact**: Loss of availability of Webshop website service. **DT1:** An attacker with the means to cause an error state in the Webshop server **V6:** Improper error handling of the Webshop server
	DR2: An attacker with the means to flood the Webshop server with multiple checkout requests and exhaust Webshop checkout service by exploiting the Webshop servers allocation of resources Without Limits or Throttling leading to the loss of availability of Webshop checkout service.	**Impact**: Loss of Availability of Webshop checkout service. **DT2:** An attacker with the means to exhaust Webshop checkout service **V7**: Allocation of Resources Without Limits or Throttling in Webshop Server
E **(Elevation of Privilege)**	**ER1**: An attacker gains admin access to Webshop by exploiting the fact that Webshop admin uses weak username and password combination, leading to loss of confidentiality of Webshop Admin username and password.	**Impact**: Loss of Confidentiality of Webshop Admin username and password Integrity of Webshop product prices **ST2:** An attacker gains admin access to Webshop. **V4:** Weak username and password combination

4.5 Summary

In this chapter, a security risk analysis is carried out, following the domain model of the ISSRM methodology. This starts out by introducing vulnerabilities as inherent characteristics of the system assets that support the business assets. These vulnerabilities are categorized using the "Seven Pernicious Kingdoms" taxonomy and labelled accordingly to be used in threat analysis. Threat analysis was carried out using the proposed STRIDE approach. This analysis considers the threat agent and the possible attack methods that exist. It also considers how they together, pose a threat to the e-commerce Webshop with each threat scenario in their STRIDE category and labelled accordingly. Knowing that elicited threats are of no importance if it does not exploit existing vulnerabilities in the system, the risk impact was analysed in the event that each elicited threat exploits system asset vulnerabilities leading to a negation of the security objectives of the business assets as well as harm to system assets.

5 Security Risk Treatment

This Chapter seeks to answer the **RQ3** – *What are the risk treatment procedures in risk management for an e-commerce system?* In order to answer this, the following questions are necessary;

RQ3.1: What is the role of security risk requirements in risk treatment?
RQ3.2: How can security requirements be applied to treat risk?

These questions will be discussed to illustrate e-commerce requirements and its elicitation, its application in the Webshop business process, and some countermeasure suggestions.

5.1 E-commerce System Requirements Definition

Knowing that the security need of an e-commerce system can be defined through the security criterion on the business assets (Confidentiality, Integrity, and Availability), these needs should be understood and correlated with the capabilities of the existing technologies [7] to make decisions concerning risk mitigations. This is where the application domain and the machine domain of an e-commerce system come to play. The application domain in the context of an e-commerce system determines the real-world purpose of the e-commerce system. Who does it provide service to? What kind of e-commerce service does it provide? Who makes sure these services are available? The machine domain, however, consists of the workings of the machine/technologies and what they have access to which could include data, devices, and applications. When the machine domain is introduced into the application domain, it fulfils the needs of the application domain. In this dynamic, aspects of the application domain allow analysts to provide proper requirement specifications for the machine domain. Security requirements will state the conditions that the machine/technologies are required to make true in order that the e-commerce system runs and functions correctly [9]. This will not include explicit statements of what needs to be implemented as this only restricts the requirements to technologies. From these requirements, the system developers can decide on what needs to be designed to run in order to meet the requirements of the application domain.

5.2 Security Requirements Elicitation

A security requirement enlists the number of conditions to fulfil to mitigate the risks and secure the e-commerce system and business assets. They define what to do to ensure secure system access, the privacy of the confidential information, what actions to be carried out to survive security attacks, proper system maintenance. For this study, a STRIDE-based security requirement elicitation is introduced. Evolving threats may not be foreseen at the point of initial requirement elicitation by the security analyst. But with the knowledge of these threats, the STRIDE based requirement elicitation method seeks to enforce security requirements that have already been developed, improve them, or introduce new requirements that will provide a more efficient security risk mitigation. The resources outlined in [20] and [26] were used to elicit security requirements for an e-commerce system specific to the risk as illustrated in Table 5 in line with STRIDE threat classes discussed in Chapter 3;

Table 5: STRIDE-based Security Requirements Elicitation

Threat type	Risk example	Security Requirement
S (Spoofing Identity)	**SR1**: An attacker with knowledge of Webshop sets up an Ad on social media with a malicious CSRF script that when clicked creates bad reviews on using the victim's account by exploiting the Webserver's inability to verify the origin of requests leading to the loss of Integrity of Customer feedback ratings. **V5:** Origin Validation Error of Webshop Server	**SR1.SReq1:** The Webshop Server shall verify the origin of requests before allowing them to use its functions. **SR1.SReq2**: The Webshop server shall protect any state-changing operation.
	SR2: An attacker with the means to compare valid sessionIDs and brute forcing to access a valid Customer session by exploiting the weak sessionID generated by Webshop Server leading to loss of confidentiality of Customer session. **V9:** Use of Insufficiently Random Values for sessionID Webshop Server	**SR2.SReq1:** The Webshop Server sessionID generation algorithm should be brute proof. **SR2.SReq2:** The Webshop shall not permit duplicate concurrent user sessions, originating from different machines
T (Tampering Data)	**TR1:** An attacker tampers with the product price by exploiting the insecurely protected unpublished Webshop API leading to the loss of Integrity of Product prices. **V2**: Insecurely protected Webshop API	**TR1.SReq1**: The Webshop shall authenticate requests to its API service. **TR1.SReq2:** The Webshop shall not rely on lack of discoverability to protect privileged functions. **TR1.SReq3:** The Webshop shall protect itself from infection by scanning the entered data.
R (Repudiation)	**RR1:** An attacker with the means to add entries to Webshop server logs to obfuscate illegal transactions on Webshop by exploiting the Improper output neutralization to Webshop server logs leading to loss of integrity of Webshop process. **V3:** Improper Output Neutralization for Webshop server logs.	**RR1.SReq1**: The Webshop shall verify that logs are protected from unauthorized access and modification. **RR1.SReq2**: The Webshop shall verify that log output is properly neutralised in log entries.
I (Information Disclosure)	**IR1:** An attacker with the means to extract Customer information from Webshop storage by sending crafted SQL injection statements through Webshop Login interface by exploiting the lack of input validation of Webshop login interface leading to loss of confidentiality of Customer information. **V1** – Lack of input validation of Webshop Login interface	**IR1.SReq1**: The Webshop shall verify that input data is canonicalized before validation. **IR1.SReq2:** The Webshop Login interface should revalidate input data in the parameterized stored procedures. **IR1.SReq3:** The Webshop shall verify that it does not output error messages containing sensitive data. **IR1.SReq4:** The Webshop shall only use parameterized stored procedures to query the storage.

	IR2: An attacker with the means to query Webshop web server for common directory names to access directory containing Customer transaction information in Webshop Storage by exploiting the improper authorization in Webshop leading to the loss of confidentiality of customer transaction information. **V8 –** Improper Authorization in Webshop.	**IR2.SReq1:** The Webshop shall verify that file names obtained from untrusted sources is canonicalized. **IR2.SReq2:** The Webshop shall verify that path data obtained from untrusted sources is canonicalized. **IR2.SReq3:** The Webshop shall constrain resources to be inaccessible by default unless selectively allowed. **IR1.SReq4:** The Webshop shall only use parameterized stored procedures to query the storage.
D **(Denial of Service)**	**DR1:** An attacker with the means to cause an error state in the Webshop server and Webshop website crashes by exploiting the improper error handling of the Webshop server leading to loss of availability of Webshop website service. **V6**: Improper error handling of the Webshop server	**DR1.SReq1:** The Webshop shall ensure that errors are gracefully handled. **DR1.SReq2:** The Webshop shall protect itself from being scanned. **DR1.SReq3**: The Webshop Admin patch Webshop components with known vulnerabilities.
	DR2: An attacker with the means to flood the Webshop server with multiple checkout requests and exhaust Webshop checkout service by exploiting the Webshop servers allocation of resources Without Limits or Throttling leading to the loss of availability of Webshop checkout service. **V7:** Allocation of Resources Without Limits or Throttling in Webshop Server	**DR2.SReq1**: The Webshop Admin shall ensure that components have limits of scale configured. **DR2.SReq2**: The Webshop Admin shall specify acceptable behaviours for when resource allocation reaches limits.
E **(Elevation of Privilege)**	**ER1:** An attacker gains access to admin interface to make product prices free by exploiting the fact that Webshop admin uses weak username and password combination, leading to loss of confidentiality of Webshop Admin username and password. **V4:** Weak username and password combination	**ER1.SReq1:** The Webshop Admin use a strong password policy. **ER1.SReq2:** The Webshop shall hide information about its Admin Interface. **ER1.SReq3:** The Webshop shall limit the number of detected attempted accesses that fail authentication requirements to 5 tries.

5.3 Security Requirements Model

Using the security requirements that have been elicited, these can be applied to the e-commerce business process model for order fulfilment developed in Chapter 3 showing where the requirements can be introduced.

Spoofing scenarios have been discussed in previous chapters where it has been illustrated how integrity and confidentiality of business assets have been negated by the described risks. The first security risk illustrated was **SR1** – An attacker with knowledge of Webshop sets up an Ad on social media with a malicious CSRF script that when clicked, creates bad reviews on using the victim’s account by exploiting the Webserver’s inability to verify the origin of requests leading to the loss of Integrity of Customer feedback ratings. This risk led to the elicitation of security requirements *SR1.SReq1* and *SR1.SReq2* as seen in Table 5. On the business process model of the Webshop, each of these security requirements has been applied to treat the risk as seen in Figure 10. The second spoofing security risk to be treated is **SR2** - An attacker with the means to compare valid sessionIDs and brute forcing to access a valid Customer session by exploiting the weak sessionID generated by Webshop Server leading to loss of confidentiality of Customer session. The security requirements for this case were *SR2.SReq1* and *SR2.SReq2* as seen in Table 5. These security requirements were applied in order to treat the risk as seen in Figure 10.

Tampering scenarios have been discussed in previous chapters by providing a risk example **TR1** demonstrating how the integrity of a business asset can be negated. The first security risk illustrated was **TR1** – An attacker tampers with the product price by exploiting the insecurely protected unpublished Webshop API leading to the loss of Integrity of Product prices. The security requirements elicitation for this case is *TR1.SReq1, TR1.SReq2* and *TR1.SReq3* applied as seen in Figure 10.

Repudiation scenario was illustrated in a risk example **RR1** – An attacker with the means to add entries to Webshop server logs to obfuscate illegal transactions on Webshop by exploiting the Improper output neutralization to Webshop server logs leading to loss of integrity of Webshop process. The *RR1.SReq1* and *RR1.SReq2* security requirements were elicited and applied as seen in Figure 10.

Information Disclosure scenarios **IR1** and **IR2** have been discussed in Table 4. For **IR1** – An attacker with the means to extract Customer information from Webshop storage by sending crafted SQL injection statements through Webshop Login interface by exploiting the lack of input validation of Webshop login interface leading to the loss of confidentiality of Customer information. The security requirements elicited to treat this risk were the *IR1.SReq1, IR1.SReq2, IR1.SReq3* and *IR1.SReq4*. These were applied as seen in Figure 10. The second risk example is the **IR2** – An attacker with the means to query Webshop web server for common directory names to access directory containing Customer transaction information in Webshop Storage by exploiting the improper authorization in Webshop leading to the loss of confidentiality of customer transaction information. The security requirements elicited to treat this risk were *IR2.SReq1, IR2.SReq2* and *IR2.SReq3*.

Denial of Service scenarios **DR1** and **DR2** have been discussed in Table 4. The first risk example **DR1** – An attacker with the means to cause an error state in the Webshop server and Webshop website crashes by exploiting the improper error handling of the Webshop server leading to loss of availability of Webshop website service. The security requirements *DR1.SReq1, DR1.SReq2* and *DR1.SReq3,* were elicited and applied in Figure 10. The second risk example discussed is **DR2** – An attacker with the means to flood the Webshop server with multiple checkout requests and exhaust Webshop checkout service by exploiting the Webshop servers allocation of resources Without Limits or Throttling leading to the loss of availability of Webshop checkout service. The security requirements *DR1.SReq1* and *DR1.SReq2* were elicited to treat the risk, applied in Figure 10.

Elevation of privileges risk example is labelled **ER1** – An attacker gains access to admin interface to make product prices free by exploiting the fact that Webshop admin uses weak username and password combination, leading to loss of confidentiality of Webshop Admin username and password. The elicited security requirements *ER1.SReq1, ER1.SReq2* and *ER1.SReq3* were applied as seen in Figure 10.

Figure 11 further illustrates how security requirements can be applied to the login procedure of the Webshop order fulfillment process with the goal to mitigate risks within that process.

5.4 Technical Security Countermeasure Selection

After requirements elicitation, the selection of countermeasures for the system is done to fulfil the elicited security requirements, and thus treat security risks. Security countermeasures are the measures taken to counter a possible threat action and should be effective as to eliminate the potential of successful threat exploitation. A significant challenge during the security risk treatment procedure is to determine the most cost-effective and appropriate set of security countermeasures. These when implemented, should mitigate risk while complying with security requirements defined by the company complying with applicable federal laws, Executive Orders, regulations, policies, directives, or standards as concerns the system [1].

As much as this is a challenge, selecting the most appropriate controls to mitigate risk is a task that requires an understanding of the existing systems in place and the business priorities. There are standards such as NIST SP 800-53 revision4 [13] that help to assist in making the appropriate selection of security countermeasures as well as the concept of baseline controls.

Countermeasures could encompass both the organizational processes of the e-commerce system and also, technical tools. An example of an organisational measure is the adoption of a secure software development methodology or some security requirements already discussed previously [2]. For technical tools, Microsoft guidelines define an initial list of countermeasures for each threat category described by STRIDE [23]. Countermeasure selection should consider the stage of system development and also the existing countermeasures such as the use of unique session per Webshop customer. Although the exact countermeasure selection for each risk is not within the scope of this research work, this consideration is only helpful to provide estimations for the final risk treatment decision taken by business stakeholders. This estimation is known as the cost of countermeasure. Table 6 illustrates some countermeasure suggestions for each STRIDE risk example in line with the security requirements elicited for the risk scenario.

Besides these countermeasure suggestions, some common web application security features for web applications should be implemented if not already done. Some of these features include but are not limited to a sufficient security policy, HTTP Protection (HTTPS), Firewall Protection, SSL Certificates, and PCI compliance checks.

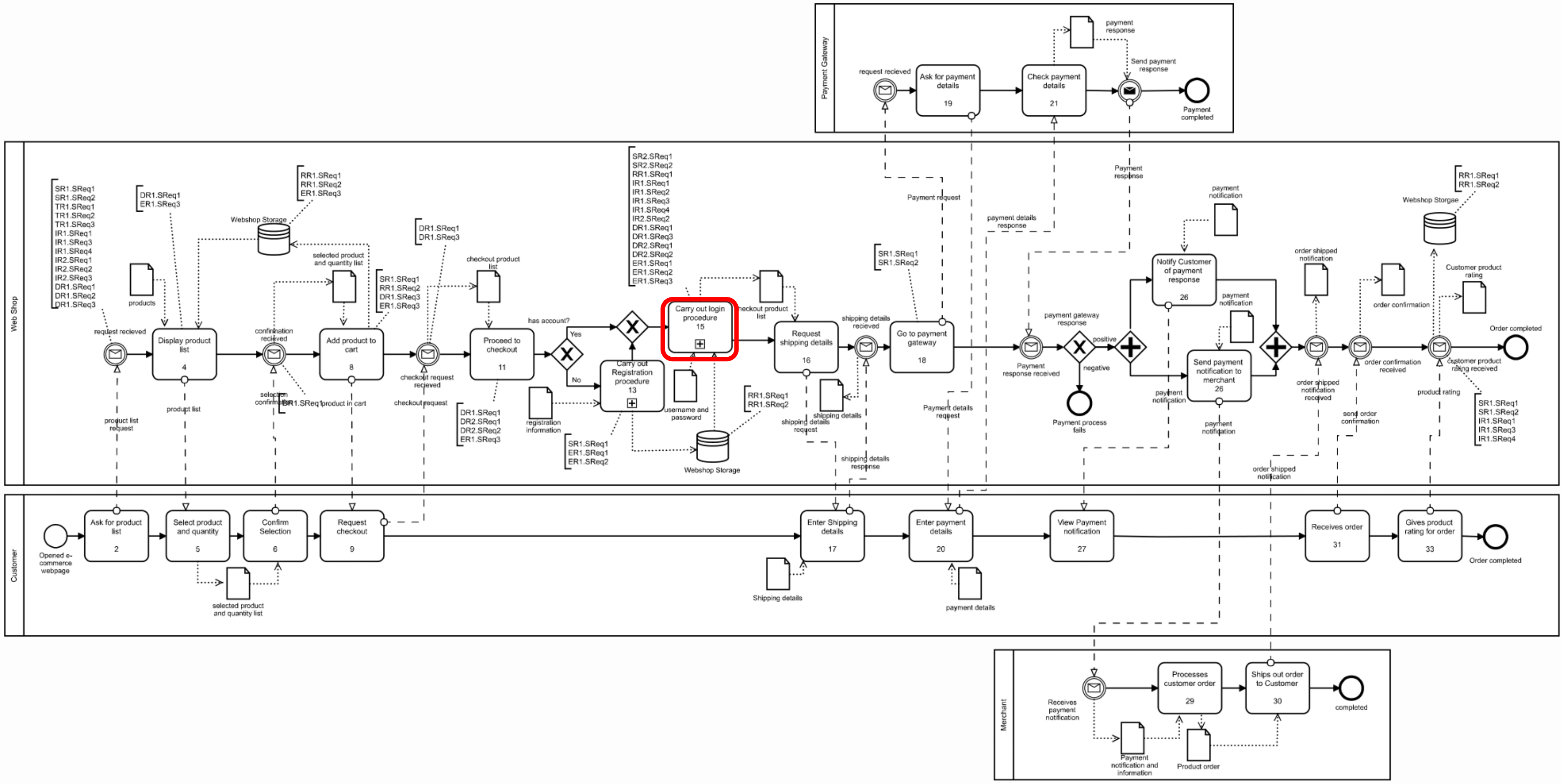
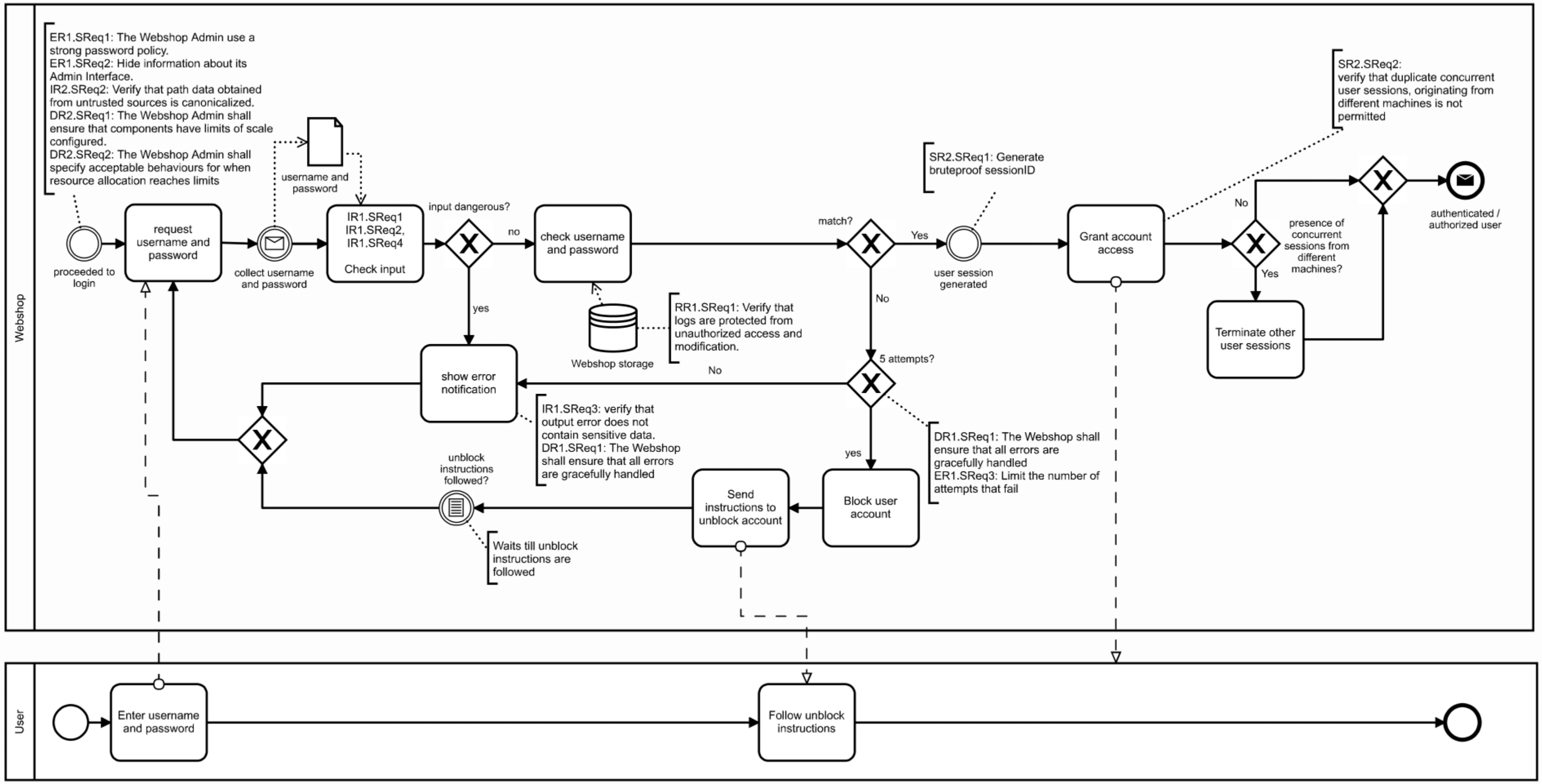


Figure 10: Security Requirements Application to E-commerce Webshop Business Process

(This is the structured perspective of the model, low fonts of labels are left intentionally)


Webshop
proceeded to login
request username and password
collect username and password
username and password
IR1.SReq1
IR1.SReq2,
IR1.SReq4
Check input
input dangerous?
no
yes
check username and password
Webshop storage
show error notification
match?
Yes
No
user session generated
Grant account access
5 attempts?
No
yes
Block user account
Send instructions to unblock account
unblock instructions followed?
No
Yes
presence of concurrent sessions from different machines?
Terminate other user sessions
authenticated / authorized user
User
Enter username and password
Follow unblock instructions

ER1.SReq1: The Webshop Admin use a strong password policy.
ER1.SReq2: Hide information about its Admin Interface.
IR2.SReq2: Verify that path data obtained from untrusted sources is canonicalized.
DR2.SReq1: The Webshop Admin shall ensure that components have limits of scale configured.
DR2.SReq2: The Webshop Admin shall specify acceptable behaviours for when resource allocation reaches limits

RR1.SReq1: Verify that logs are protected from unauthorized access and modification.

IR1.SReq3: verify that output error does not contain sensitive data.
DR1.SReq1: The Webshop shall ensure that all errors are gracefully handled

Waits till unblock instructions are followed

SR2.SReq1: Generate bruteproof sessionID

DR1.SReq1: The Webshop shall ensure that all errors are gracefully handled
ER1.SReq3: Limit the number of attempts that fail

SR2.SReq2: verify that duplicate concurrent user sessions, originating from different machines is not permitted

Figure 11: Security Requirements Application to the Carry Out Login Procedure of Webshop

Table 6: Security Countermeasure Suggestion

Threat type	Security Requirement	Countermeasure suggestions
S (Spoofing Identity)	**SR1.SReq1:** The Webshop Server shall verify the origin of requests before allowing them to use its functions. **SR1.SReq2**: The Webshop server shall protect any state-changing operation.	Use cryptographic tokens generated at each request. Enable optional HTTP Referrer header.
	SR2.SReq1: The Webshop Server sessionID generation algorithm should be brute proof. **SR2.SReq2:** The Webshop shall verify that it does not permit duplicate concurrent sessions, originating from different machines. **SR2.SReq3:** The Webshop shall hide sessionID data.	Use a potent source of randomness with adequate length to generate a session ID Protect authentication cookies with Secure Sockets Layer (SSL). Design: Make code changes that prevent multiple concurrent sessions from different machines.
T (Tampering Data)	**TR1.SReq1**: The Webshop shall authenticate requests to its API service. **TR1.SReq2:** The Webshop shall not rely on lack of discoverability to protect privileged functions. **TR1.SReq3:** The Webshop shall protect itself from infection by scanning the entered data.	Use OAuth 2.0 authentication protected through SSL/TLS. Malware scanning solution
R (Repudiation)	**RR1.SReq1**: The Webshop shall verify that logs are protected from unauthorized access. **RR1.SReq2**: The Webshop shall verify that logs are protected from unauthorized modification. **RR1.SReq3:** The Webshop shall store tamper-proof records of server logs **RR1.SReq4:** The Webshop shall verify that log output is properly neutralised in log entries.	Design: Make code changes that use input validation before writing to the server log. Design: Make design code changes that validate log data before it is output. Implement tamper-proof technologies for web server logs
I (Information Disclosure)	**IR1.SReq1**: The Webshop shall verify that input data is canonicalized before validation. **IR1.SReq2:** The Webshop Login interface should revalidate input data in the parameterized stored procedures. **IR1.SReq3:** The Webshop shall hide information about itself outputting error messages. **IR1.SReq4:** The Webshop shall only use parameterized stored procedures to query the storage.	Design: Make code changes to implement strong input validation Design: Make code changes to use parameterized queries or stored procedures Design: Use of custom error pages coupled with input validation to inform about an error without disclosing sensitive information.
	IR2.SReq1: The Webshop shall verify that input obtained from untrusted sources is canonicalized. **IR2.SReq2:** The Webshop Admin shall constrain resources to be inaccessible by default unless selectively allowed.	Design: Make code changes to verify that file names and path data obtained from untrusted sources is canonicalized Design: Make changes to ACLs Use strong authorization.

D (Denial of Service)	**DR1.SReq1:** The Webshop shall ensure that errors are gracefully handled. **DR1.SReq2:** The Webshop shall protect itself from being scanned. **DR1.SReq3**: The Webshop Admin patch Webshop components with known vulnerabilities.	Ensure that sensitive server information is not exposed in the event of being scanned. Promptly patch software components. Design: Ensure code level error handling mechanisms are in place and adequate. Replace components that cannot be patched. Configure the firewall to block scanning activity.
	DR2.SReq1: The Webshop Admin shall ensure that components have limits of scale configured. **DR2.SReq2**: The Webshop Admin shall specify acceptable behaviours for when resource allocation reaches limits. **DR2.SReq3**: The Webshop shall uniformly throttle requests.	Ensure that the protocols used have specific limits of scale configured. Make code changes to make it more challenging to consume resources more quickly than they can be freed. Use resource and bandwidth throttling techniques.
E (Elevation of Privilege)	**ER1.SReq1:** The Webshop Admin implement a strong password policy. **ER1.SReq2:** The Webshop shall hide information about its Admin Interface. **ER1.SReq3:** The Webshop shall limit the number of detected attempted accesses that fail authentication requirements to 5 tries.	Alternatively, strong passwords for Admin users can be automatically generated. Make code changes to limit the number of detected attempted accesses that fail authentication requirements to 5 tries. Make code changes to remove information concerning admin interface.

5.5 Summary

In this chapter, the concept of security treatment was introduced. This included an understanding of security requirements, its meaning and its importance as the listing of conditions required to be made true by the system in order to ensure security. The security requirements appropriate for each risk scenario were identified and listed. These requirements were further applied to the order fulfillment business process model which illustrating where these security requirements may apply. Also, suggestions were made on possible countermeasures that can be taken (in line with the security requirements) to reduce security risk within the risk scenarios.

6 Security Risk Measurements

This chapter seeks to answer further, **RQ3** – *What are the risk treatment procedures in risk management for an e-commerce system?* This is done by answering the question;

RQ3.3: How can security risk be measured for risk treatment implementation?

This sub-question will illustrate how security risks can be measured for the purpose of risk treatment implementation.

6.1 Security Risk Metrics

To make the correct response to risk the following parameters need to be taken into account;

- The cost of responding to risk (i.e. cost of insurance in the case of risk transfer and the cost of implementing control measures in the in the case of risk reduction)
- The importance of the risk to be addressed
- The effectiveness of the risk response (seen in potential risk reduction level)

Security risk measurements help to analyze the possible cost of countermeasures selected to treat the risk, the potential risk reduction level and make treatment decisions. Security risk measurements are done using metrics that estimate the value of the security risk concepts. The value metric estimates the security need [20] of each business asset in terms of confidentiality, integrity, and availability. This metric expresses the importance and the application of the security criterion in regards to the business asset and according to the domain model, is an attribute of the security objective.

The risk is estimated using a risk level metric [20] which depends on the event *potentiality* and the *impact level*. Because an event comprises of the security *threat* and *vulnerability* of the system asset, thus the event *potentiality* can be estimated through the *threat likelihood* and *vulnerability level*. Risk-treatment can be estimated first in terms of *risk reduction* performed and then in terms of *cost incurred* in implementing security controls. The implementation of these security metrics would result in a qualitative analysis of security risk reduction levels of the STRIDE-based risk examples. Business assets can be estimated in terms of a *value* which could be monetary, in hours, and in rate per hour. The *value* of the business asset is used as input to estimate the security need.

6.2 Security Risk Metric Example

A security risk example is used to illustrate the security risk metric estimations.

DR1 - An attacker with the means to cause an error state in the Webshop server and Webshop website crashes by exploiting the improper error handling of the Webshop server leading to loss of availability of Webshop website service. For business asset metric, the business asset value of the Webshop checkout service is derived and presented at different levels from low to high (1 – 3) as seen in Table 6.

Table 7: Business Asset Value

Business Asset Value: Webshop checkout service	
Value Estimate	**Description**
3 – High	Checkout service should be available 99.9%
2 – Normal	Checkout service should be available for up to 90%
1 – Low	Checkout service should be available for up to 80%

In this next case, the security criterions are considered to find the possible security need for the security risk and this is done by carrying out an analysis on the Confidentiality, Integrity and Availability of the Webshop checkout service at different levels (0 – 3). Table 8 shows each of these levels and their effects (if any) on the Webshop checkout service business asset.

Table 8: Security Objective Metrics

Security Objective			
	Need for Confidentiality	Need for Integrity	Need for availability
0	No need for confidentiality	No need for integrity	No need for availability
1	-	-	Checkout service should be available for up to 80%
2	-	-	Checkout service should be available for up to 90%
3	-	-	Checkout service should be available 99.9%

The security need(s) of the Webshop checkout service have been defined for the appropriate security criterion. With the threats relevant to the system assets concerned with the risk (Webshop shopping cart component and Webshop Server) already discussed in the previous sections, the threat likelihood can be measured from 1 – Low, 2 – Medium, 3 – High as seen in Table 9;

Table 9: Threat Likelihood

Threat likelihood	
1	Low likelihood of attacker's successful implementation of the attack method (means, opportunity and competence).
2	Possible likelihood of the attacker's successful implementation of the attack method.
3	High likelihood of the attacker's successful implementation of the attack method.

The threat is associated with the *improper error handling of the Webshop server* vulnerability that could be exploited by the attacker The level of vulnerability can be measured from 1 – Low, 2 – Medium, 3 – High as seen in Table 10;

Table 10: Vulnerability Level of System Assets

Vulnerability level	
1	Low vulnerability level with appropriate security measures in place to protect against risk.
2	Medium vulnerability level with little security measures in place to protect against risk.
3	High vulnerability level with inadequate security measures in place to protect against risk.

The event potentiality of the risk can be calculated as;

Potentiality = threat likelihood + vulnerability level – 1

This is derived from the event matrix of threat *likelihood* and *vulnerability level*. The impact level of the risk is based on the security need derived from the security criterion of the Webshop checkout service. This will be the value of the highest metric for the security need.

The risk level can then be calculated as ;

*Risk level = risk event potentiality * impact level*

This is derived from the risk matrix of *event potentiality* and *impact level*. The cost of countermeasure can be introduced in terms of levels low, medium, high.

Table 11: Cost of Countermeasure Metric

Cost of countermeasure	
1	Little or no cost of control implementation in order to treat risk.
2	Medium cost of control to implement in order to treat risk.
3	High cost of control to implement in order to treat risk.

From Table 10, the *vulnerability level* selected for DR1 is level 3 as there are inadequate security measures in place to protect against risk in the event that it occurs. The threat *likelihood* chosen was a level 3 as there is a high likelihood of the attacker’s successful implementation of the attack method that leads to successful exploitation of the *improper error handling of the Webshop server* vulnerability. The *event potentiality* was calculated according to the already provided formula and the *impact level* was chosen as a level 3 because the highest security need of the concerned security criterion was of a level 3. This is illustrated in Table 12.

The risk metric illustration will be carried out for other risks in the STRIDE Table 4, to arrive at Table 13 illustrating the risk metric for risk scenarios before and after risk treatment. The metric calculations remain the same but may differ for business asset value estimations. However, its levels of 3 – high, 2- medium and 1- low, still remain the same. To summarize, the risk event potentiality, risk impact level, and risk level metrics are then calculated as follows according to the GQM framework application on the ISSRM domain [21]:

- Risk event = *threat likelihood* + *vulnerability level* − 1
- Impact = maximum value of the *security criterion*

- Risk level = *risk event* * *impact*.
- Maximum-risk level = (3 + 3 − 1) * 3 = 15
- Minimum-risk level = (1 + 1 − 1) * 0 = 0
- Risk reduction level = Risk level 1 − Risk level 2

The minimum risk level obtainable is 0, and the maximum risk level obtainable is 15. These specify the boundaries of the risk. Risk level 1 is calculated with no countermeasures to the risk in place and then Risk level 2 is calculated with the appropriate security countermeasures applied. The risk reduction level is then calculated with the collated data for the risks in Table 4 illustrated in Table 13.

6.3 Security Trade-off Analysis

The required effort for risk response (in the case of mitigation or transfer) will likely exceed available resources. In this case, some risk trade-off analysis is required. A security trade-off analysis can be done in this case [21] to place security requirements to be plotted in graphs with quadrants offering three possible options labeled as low - 1, medium – 2 and high – 3;

- High (Quick wins): This case includes efficient and effective responses to risks.
- Medium (Business case to be made): This case includes more difficult responses to lower risk that requires careful analysis and management decisions.
- Low (Deferral): This case includes costly responses to lower risks.

A trade-off analysis is done based on;

- the value of the business asset,
- counter-measure cost and
- risk reduction level

The metrics in the last three columns collated in Table 13, were used to create three graphs. The first graph is the risk reduction level vs. business asset value, next is the risk reduction level vs. cost, and finally the cost vs. business asset value. Each graph is divided into four quadrants and the priority on each with each quadrant is illustrated in Table 14: Determining Risk Priority.

In Figure 12: Risk reduction level vs. Business Asset Value, the desired situation is one where an asset of high business value has a high risk reduction level value which is identified in the quadrat having SR2, TR1, DR1 and ER1 and therefore represents high priority. Medium priority risks represent those with high business asset value and low risk-reduction level (as seen in risks IR2, RR1, DR2), and those with high risk reduction level and low business asset value (as seen in risk IR1). However, the least desired situation, in this case are risks with low business asset value and low risk reduction level (as seen in risk SR1).

Table 12: DR1 Security Risk Reduction Level Metric

<table>
<tr><th colspan="3">Business asset</th><th colspan="5">DR1</th><th colspan="6">Security Requirements</th></tr>
<tr><td colspan="3" rowspan="2">Webshop website service</td><td colspan="5">An attacker with the means to cause an error state in the Webshop server and Webshop website crashes by exploiting the improper error handling of the Webshop server leading to loss of availability of Webshop website service.</td><td colspan="6"><b>DR1.SReq1:</b> The Webshop shall ensure that errors are gracefully handled.
<b>DR1.SReq2:</b> The Webshop shall protect itself from being scanned.
<b>DR1.SReq3:</b> The Webshop Admin patch Webshop components with known vulnerabilities.</td></tr>
<tr><td colspan="5">Before treatment</td><td colspan="4">After treatment</td><td>Risk reduction level</td><td rowspan="2">Cost of counter-measures</td></tr>
<tr><td>Value</td><td colspan="2">Security need</td><td>Vulnerability level</td><td>Threat likelihood</td><td>Event potentiality</td><td>Impact level</td><td>Risk level 1</td><td>Vulnerability level</td><td>Threat likelihood</td><td>Event potentiality</td><td>Risk level 2</td><td>R1 – R2</td></tr>
<tr><td rowspan="3">3</td><td>C</td><td>0</td><td rowspan="3">3</td><td rowspan="3">3</td><td rowspan="3">5</td><td rowspan="3">3</td><td rowspan="3">15</td><td rowspan="3">1</td><td rowspan="3">2</td><td rowspan="3">2</td><td rowspan="3">6</td><td rowspan="3">9</td><td rowspan="3">2</td></tr>
<tr><td>I</td><td>0</td></tr>
<tr><td>A</td><td>3</td></tr>
</table>

Table 13: Risk Metrics Before and After Risk Treatment

	Business Asset Value	Before Treatment					After Treatment				Risk reduction level	Cost of counter-measure
		Vulnerability level	Threat likelihood	Event potentiality	Impact level	Risk level 1	Vulnerability level	Threat likelihood	Event potentiality	Risk level 2		
SR1	2	2	3	4	3	12	1	2	2	6	6	3
SR2	3	3	3	5	3	15	1	2	2	6	9	2
TR1	3	3	2	4	3	12	1	1	1	3	9	3
RR1	3	2	2	3	3	9	1	1	1	3	6	2
IR1	2	3	3	5	3	15	1	2	1	3	12	1
IR2	3	2	3	4	3	12	1	2	2	6	6	2
DR1	3	3	3	5	3	15	1	2	2	6	9	2
DR2	3	2	2	3	3	9	1	1	1	3	6	3
ER1	3	3	2	4	3	12	1	1	1	3	9	2

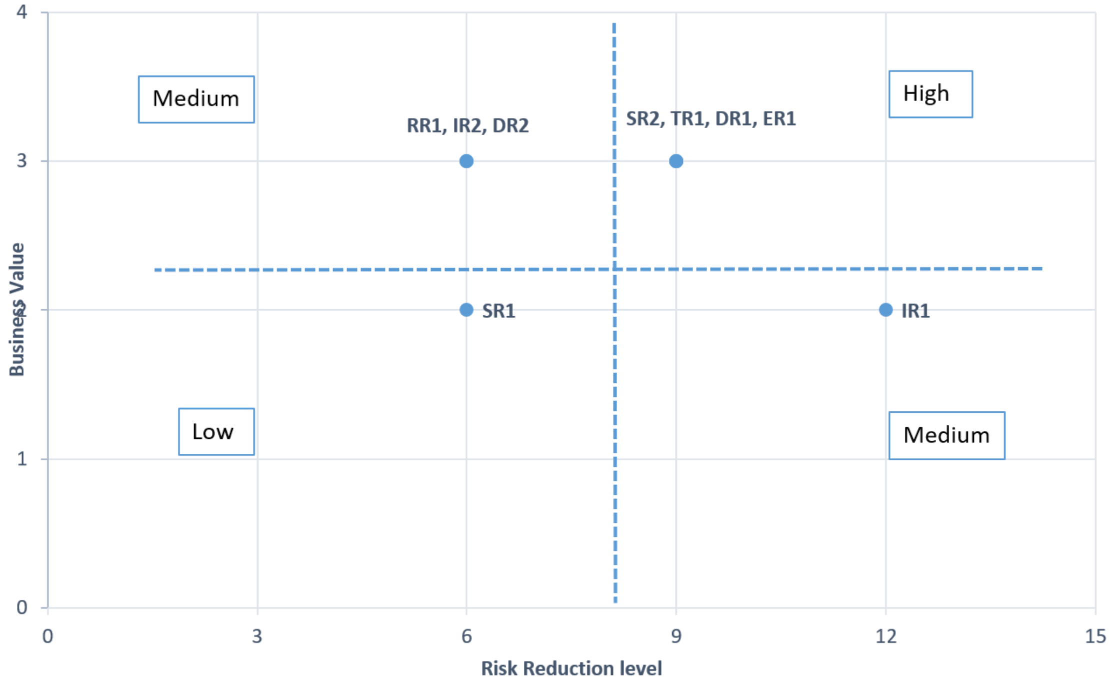


Figure 12: Risk reduction level vs. Business Asset Value

In Figure 13, the desired situation is one where there is a low countermeasure cost with a high risk reduction value, identified by the quadrant having risks SR2, DR1, IR1, ER1 and is thus represented as having high priority. Medium priority is found in quadrats having a high cost of countermeasure value with high risk reduction levels (as seen in risk RR1) and a low countermeasure cost with low risk reduction value (as seen in risk RR1, IR2). The low priority risks can be identified in the quadrant having a high countermeasure cost and a low risk reduction level value and is seen in the risks SR1, DR2.

In Figure 14, the risks of high priority are in the quadrant having low cost of countermeasure with high business asset value having risks SR2, RR1, IR2, DR1, ER1. Medium priority is found in quadrants having high value business assets with a high cost of countermeasure (as seen in risks TR1, DR2) and a low-value business asset combination with low countermeasure cost (as seen in risks IR2). The least desired situation is one of low business asset value with a high countermeasure cost as seen in risks SR1.

Table 14 illustrates the results of the security risk tradeoff analysis derived from combining the priority levels of low, medium and high from the graphs of Figure 12, Figure 13 and Figure 14 where a value of 3 is assigned to high priority risks, 2 assigned to medium priority risks and 1 assigned to low priority risks. When these values are collated from all three figures, an overall priority can be estimated that depends on the values of business asset, countermeasure cost and risk reduction level. These values in Table 14 are presented in order of priority from High to Low.

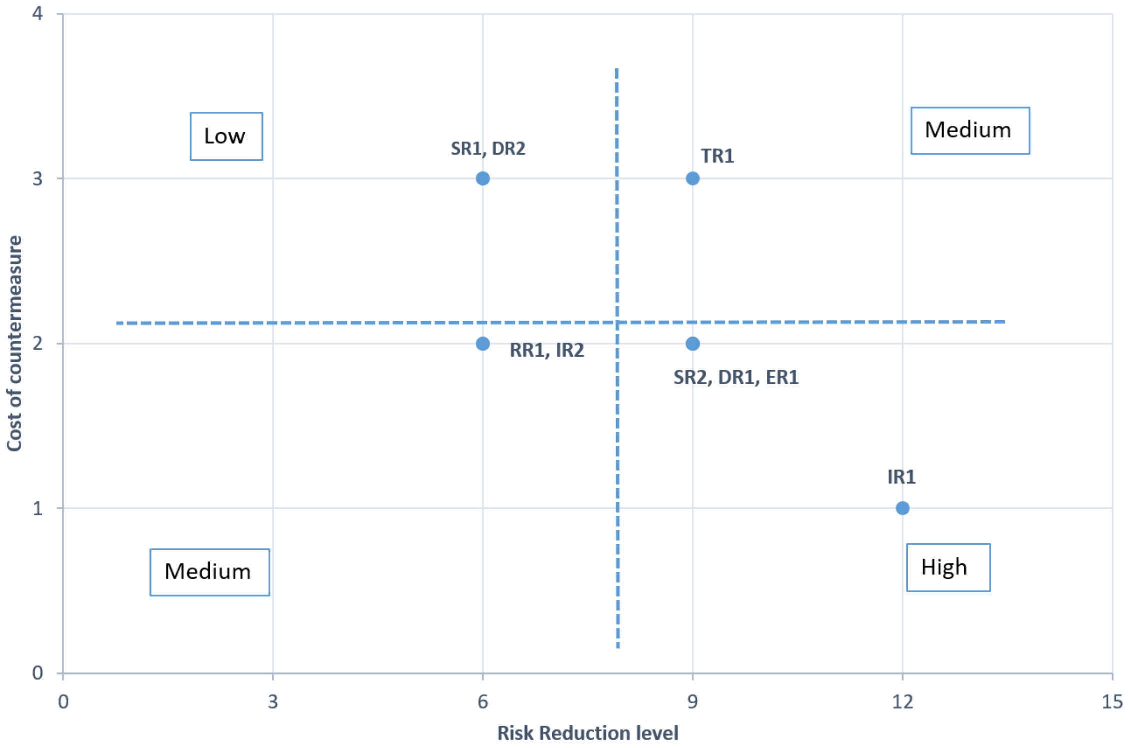


Figure 13: Risk Reduction Level vs. Cost of Countermeasure

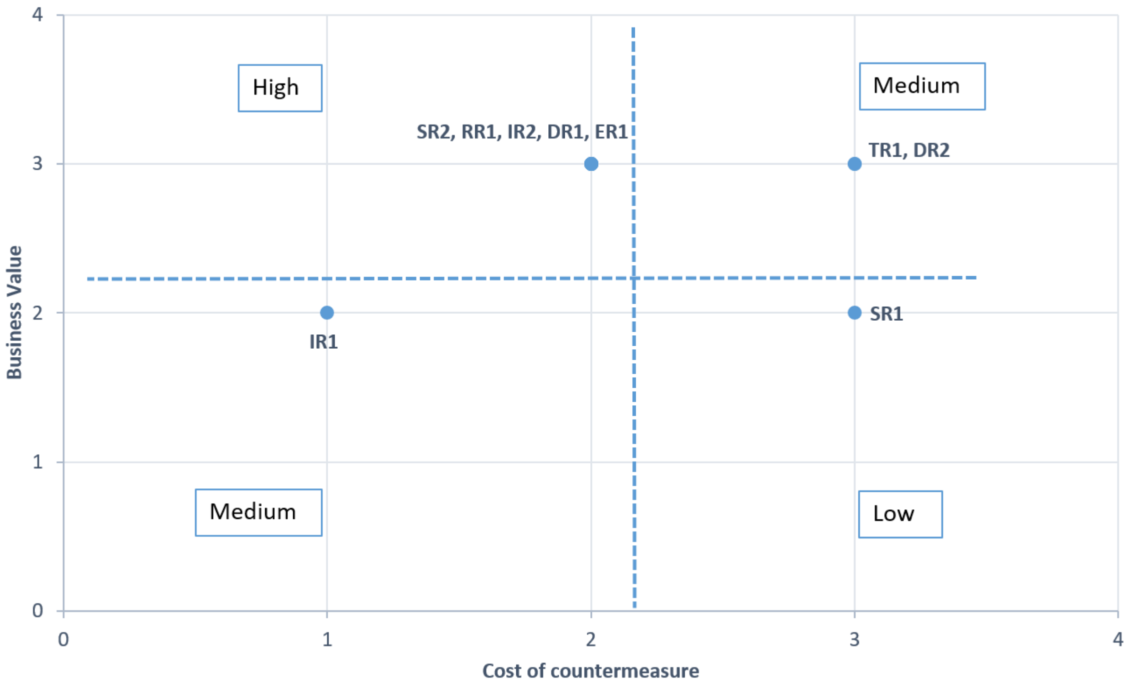


Figure 14: Cost of Countermeasure vs. Business Asset Value

From the collation, the following can be seen;

- high priority are those with the highest values – 9 (SR2, DR1, ER1),
- medium priority are those with values 7 (TR1, RR1, IR1, IR2) and
- low priority are those with values below 7 (SR1, DR2)

A trade-off analysis table is derived for better risk priority communication. Now, security countermeasures for the Webshop can now be implemented using the relevant standards and resources as guidance. A security risk re-analysis is advisable although not covered by this research work as a two security analysis procedures will be challenging to carry out within the time frame.

Table 14: Determining Risk Priority

	Business Value – Risk Reduction Level	Risk Reduction Level – Cost of Countermeasure	Business Value – Cost of Countermeasure	Priority	
SR2	3	3	3	9	High priority
DR1	3	3	3	9	High priority
ER1	3	3	3	9	High priority
TR1	3	2	2	7	Medium priority
RR1	2	2	3	7	Medium priority
IR1	2	3	2	7	Medium priority
IR2	2	2	3	7	Medium priority
DR2	2	1	2	5	Low priority
SR1	1	1	1	3	Low priority

6.4 Summary

This chapter goes further to provide guidance on security risk treatment decisions by the introduction of security risk measurements. These security risk measurements offer useful estimations on the value of business assets, countermeasure cost and the potential risk reduction level following a risk treatment decision. Security risk measurements also pave the way for useful risk trade-off analysis that help in deciding which risks are of high priority to treat first in relation to the other security risks.

7 Validation of Security Risk Management Procedure

This chapter discusses the validation procedure by expert analysis for the thesis work. It discusses the expert backgrounds, a description of the procedure, the results of the validation done and the threats to validity. Validation is essential for proffering correctness of the thesis content and the usefulness of the risk management procedure to the body of knowledge.

7.1 Expert Background

The expert participants were purposefully selected based on their experience with each of the different stages of the risk management procedure. With the expert's backgrounds, it was expected that they would have the most valuable information and present valuable feedback on this thesis research. A total of seven (7) experts took part in this study. These experts were IT professionals (2) and those with Business Information technology (5) background. Some experts with business IT background had a lot of business analytical background as well and qualified to be both in the category of the business analyst as well as the business IT. This selection was made in such a way that the results of the validation will as much as possible, uphold correctness on both IT and business aspects of this thesis work as seen in Figure 15;

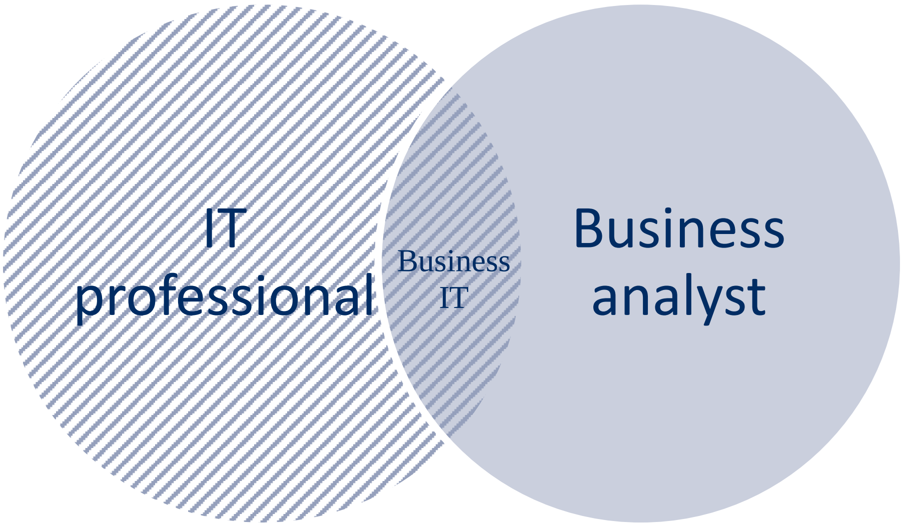


Figure 15: Concept of Expert Background for Validation

The experience of the IT professional experts are as follows;

Expert 1: QA Team Lead with 10+ years experience with Software development and Testing (including 2years experience with e-commerce related software development)

Expert 2: Development Team Lead with 10+ years experience in Software development (including 3years experience with e-commerce related software development)

The experience of the Business Information technology experts are listed as follows,

Expert 3: Director of Cybersecurity with 26+ years in IT governance and business IT related roles.

Expert 4: Team Lead for Security Operations Centre with 20+ years experience in IT governance and business IT related roles.

Expert 5: Cybersecurity engineer with 7+ years experience including Business IT governance and e-commerce related software development.

Expert 6: Cybersecurity engineer with 7+ years experience including Business IT and IT Infrastructure management.

Expert 7: Technical product specialist with 4+ years IT experience including business process management research.

Within their expertise, they fulfil high-level professional roles and other managerial roles and represent the those of whom this thesis research will be useful to.

7.2 Description of Validation Procedure

Each participant was invited via e-mail to participate in the validation procedure of the research work, explaining the thesis goal and providing details about the methodologies, methods, and procedures used. With each expert, an introduction to the thesis idea and structure of work was conducted. This was done by personal meetings, skype meetings and via email (sending a summary of work done). This resulted in the decision from each participant to continue with the validation procedure based on time constraint and experience with the thesis research field. Further discussions took place in multiple physical and Skype interviews with each of the participants.

These interviews addressed the Chapters 3, 4 and 5 from the viewpoint of its understandability, structure and flow around three open questions:

- Is the structure of the procedure understandable?
- Do you agree with the relevance of the business and system assets, vulnerabilities and threats?
- Do you agree with the models of the Webshop example?
- Do you agree with the usefulness of the STRIDE approach to security risk management taken?
- Are any specific parts of the security risk management procedure missing?

During the interview, specific notes were taken including the various opinions, suggestions, and recommendations. Some changes were made to explain aspects of the procedure which were lacking in relation to other parts, others to the models used to represent the security risk management procedure and so on. The goal of the new changes was to represent the opinions and ideas expressed by the experts as accurately as possible as it applied to the thesis research.

Finally, another set of meetings were carried out on the figures that were developed for the security risk treatment metrics. In these meetings, questions were asked to verify the metrics to the following, including if they agreed with it or not:

- Business Asset value
- Security Objective (CIA) value
- Threat likelihood value
- Vulnerability value
- Cost of countermeasure value

Each of the opinions of the security experts was taken into consideration, and at the end, a final thesis research document was generated.

7.3 Results of Validation Procedure

This section contains a documentation of the validation results that follow the expert validation on each step of the risk management procedure from the asset-related concepts to the risk-related concepts and then the risk treatment-related concepts of the Webshop.

7.3.1 Validation of Asset-related Concepts

The assets-related concepts involved discussions made in Chapter 3 concerning e-commerce security assets (business and system assets) related to the scenario of order fulfilment in a Webshop as well as the order fulfilment business process model. The open questions were asked as explained in the description. The respondents agreed to the fact that the explanations given and relevance of the assets were understood based on the scenario in use. In this case, scopes may widen if other processes in the Webshop was considered or if each process was expanded further. The BPMN model for the Webshop Order fulfilment process was validated for syntactic and logical correctness by the experts. Some corrections were offered by Expert 6, stating that "*proper labelling of control flows ensures consistency and easy readability and understandability of your model". These corrections were made and submitted for another review which was successful. The model was also found to be a general flow of order fulfilment, with an emphasis made by Expert 1 on the fact that "… *based on the business design, some order fulfilment processes may vary. But, as the keyword here is "generic", this model is appropriate".*

7.3.2 Validation of Risk-related Concepts

The risk-related concepts involved in this validation part involves research made in Chapter 4 concerning vulnerabilities of the system assets elicited in Chapter 3, the threats that arise from the presence of these vulnerabilities, the resulting impact of successful exploitation and the resulting security risk to the Webshop. The relevance, understandability, and correctness of each concept will be considered.

After a discussion explaining the concepts, the open questions were asked as explained in the description. The correctness and relevance of the vulnerabilities were first discussed. Here there was an agreement on their relevance, but a disagreement was raised by Expert 4 concerning the inclusion of threat examples at this stage, stating that "*introducing threat examples when the concept of threats have not been discussed just confuses those reading".* The advice presented was to "*stick to the listing of vulnerabilities and not jump into listing* *threat examples at this stage"*. This was corrected in the thesis work as this opinion was agreeable.

Next, the STRIDE threat scenarios were discussed. Here there was also an agreement in the logical flow from vulnerability to threat, and the labels that help to connect them easily when tracing vulnerability to threat. The procedure was seen to be understandable by the experts as Expert 3 had commended that "… *the line of thought and the process was easy to follow"*. Although the business-oriented experts could not fully understand the technical details of the threat, the sense of threat was said to be understood by reading the threat statement.

Then the final risk scenarios were discussed. There was an agreement on the relevance of the risk scenarios developed, however Expert 1 commented that "… *more malicious scenarios could have been developed"* but he went on to comment that "*the risk scenarios here are of course still malicious and stand a risk of affecting the Webshop in damaging ways as well*". Expert 5, when asked about the level of maliciousness of the risk scenarios, was indifferent to the claim of the scenarios not being malicious enough but also suggested basing these scenarios on information from well-known databases such as CAPEC, OWASP and CWE [5]. This suggestion was taken into account as these information databases also held information vital to the risk measurement procedure.

The organisation of each risk scenario according to the STRIDE threats listed in the previous section was commended as well as the labels developed that helped tracking of each part of the risk statement to its corresponding threat and vulnerability. In summary, the STRIDE procedure, its presentation and the correctness and relevance of each of the sections were agreed with and commended. The suggested corrections were carried out and the final work submitted to the experts again for a final review which returned positive feedback. Here no models were discussed.

7.3.3 Validation of Risk Treatment-related Concepts

The risk treatment-related concepts to be validated includes work done in Chapter 5 concerning the security requirements elicited to mitigate security risk scenarios discussed in Chapter 4. The logical and syntactic accuracy of the illustration of these security requirements as well as the security risk trade-off analysis procedures is evaluated with the open questions asked.

First, there was an overall agreement on the importance of security requirements in risk mitigation as well as an agreement on the security requirements elicited for each risk scenario. However there were some doubts on whether these requirements will undoubtedly aid in treating the risks, some suggestions were made on requirements elicited which were taken into account. One suggestion was made by Expert 2 concerning security requirement dependencies, stating that "*... as each requirement per risk scenario is not being implemented on a separate system, each requirement will somehow have relationships to one another.*" This situation was advised to be considered during requirement elicitation phase.

Each of the security requirements to be implemented as controls on the system was shown including the example model for the *carry out login procedure*. The experts assessed this model, and there were suggestions made by Expert 4 & 6 to simplify the model. Expert 4 stressed on the fact that the model had to be "*… specific with also the countermeasure implementations on the diagram. Leaving it open for interpretation will not pass across the intended message of the application of security requirements because security requirement application is the application of actual controls and not the idea of one"*. This opinion was considered, and the model simplified, corrected and sent for review two more times before an agreement was reached.

In another set of meetings the metric values used for the security risk treatment section was discussed. Here, the values assigned to the business assets, security objective, vulnerability level, threat likelihood, and the cost of countermeasure were discussed in-depth. For the business asset metric, many factors were considered. There was a collective opinion that a quantitative value is difficult to come up with as it will involve many things such as average sales, customer action on the event of risk, time to recover, normal expected outage time, the necessity of the product, if it is a specialised product, and so on. The final decision made was suggested by Expert 3 to "*… not include any quantitative analysis. With the different factors to be considered when carrying out quantitative analysts, this would prove out of scope to the research work at hand and will instead raise confusion*". As for the metrics relating to vulnerability and threats, a suggestion was made to cross-check these estimations with estimations made on credible databases such CAPEC, OWASP or CWE. As regards to cost of countermeasure metrics, Expert 6 suggested that *"... it would be nice to have an idea of the countermeasures considered in this metric. Maybe include an example before and then it can be known that as such, this metric could be Low, Medium or High depending on the resources available to the e-commerce system*". There were no contentions on the risk reduction level as this was as a result of calculations based on vulnerability levels, impact and security objective value and as such cannot be subject to opinions at this stage. The security trade-off analysis was commended, illustrating what is of high priority.

The results of the validation brought forth positive feedback. There was a collective agreement on the security risk management procedure and opinions provided on each concept were positive as well. The procedure was seen to be understandable, clear, easy to follow and relevant to the system. Expert 7 commented that "*... using a simulation tool would have also been a great addition to the validation procedure*". This was a valuable opinion, but with the time constraints at this stage, nothing significant could be done in this regard.

7.4 Threats to Validity

The major threat to the validity of this research work is the subjectivity of expert validation opinions on the proposed approach. This is because the approach has not undergone live e-commerce system tests to conclude on its validity so its efficacy may remain subjective until implementation of this approach is done. Although there were procedures to carry out this approach on a live e-commerce system, doing this would not be productive within the set time frame. Also, the experts chosen are knowledgeable in this field and so can provide opinion and suggestion feedback that is relevant.

The completeness of the open questions asked during the validation procedure was another point of doubt that posed a threat to validity. Were the right questions asked? Were the questions complete? Were the questions appropriate enough to validate the research procedure?

Also, as not all of the expert opinions were relayed into refining the proposed approach, a threat lies in the fact that the method used to decide what opinion was to be accepted and which was to be ignored is still subjective.

7.5 Summary

This chapter discusses the validation procedure used in the thesis research. This procedure follows expert validation process discussing questions that help to conclude on the relevance, usefulness, and understandability of the STRIDE approach in security risk management. The results of the validation procedure were positive with commendations on the systematic structure of the work done. Many suggestions were offered and although valuable, not all could be considered as some were either out of scope or not time efficient.

Some threats to validity existed which bordered around subjectivity of the views and opinions of the experts as well as doubt on the appropriateness of the validation questions asked and the appropriateness of the background of the experts selected.

8 Summary of Work

This final chapter presents a summary of the research work carried out including the limitations of the research, the answer to the research questions for this work, conclusions of the research work and some proposals for future work.

8.1 Limitations of Research

This research work concentrated on only one type of e-commerce system which is the business-to-customer e-commerce system. As explained in the scope, there are other types of e-commerce systems not considered in this research work. We also concentrate on the order fulfilment process of a B2C e-commerce system which limits the business view of the applicability of the approach. The case-study used for this security risk management process was from a generalisation of the concepts of a standard e-commerce system following research on a of popularly used e-commerce systems.

Also, with the illustration of security metrics for risk treatment, it is acknowledged that such metrics are subjective and are highly business specific. The research work only provides a general estimation for risk metric values for its calculations.

8.2 Answer to Research Questions

The answers to the research questions in this master thesis have been provided as follows;

Research Question 1: How can relevant assets for an e-commerce system be identified?

The relevant assets for an e-commerce system are identified by describing and modelling the operation of the business processes that aim to achieve the business goal. A study of e-commerce retail sites was carried out to understand the general flow of the e-commerce application and model its business process. The business process selected in this case was the order fulfilment process, and a model describing this process was instrumental in revealing assets of the system. The BPMN modelling language was used to identify and elicit assets in an e-commerce system. The process workflow included the *Product Catalog process*, *Shopping Cart process*, *Payment process* and the *Shipping process* which together form the *order fulfilment process*. Using this model, both business assets and system assets that support the business assets are illustrated implicitly or explicitly. The assets discovered were discussed in Section 3.3 and 3.4. The assets that pose security concerns to the e-commerce systems are both the system assets as well as the business assets. The system assets are characterised by having vulnerabilities which can be exploited leading to security risks in the e-commerce system. These system assets require some countermeasure implementation to fix the vulnerabilities that they contain.

The business assets also pose security concerns by their value to attackers as seen in the security criterions assigned to each business asset. Thus the assets elicited in Section 3.3 and 3.4 pose security concerns in an e-commerce system. As illustrated in this thesis work, risk management to ensure security in the system is based on the assets that have been identified and the threats relevant to these assets. If there is no proper asset identification done, security risk management procedure will be lacking and have an incorrect scope. Also, without the identification of assets, vulnerabilities cannot be discovered, and thus relevant threats to the system cannot be known. As illustrated in Chapter 3 of the research work, assets listed here provided grounds for vulnerability elicitation which continued into the risk analysis stage.

Research Question 2: What are the security threats as well as its resulting risk to an e-commerce system?

Security threats to an e-commerce system exist in a wide variety ranging from common web application threats to threats specific to customer privacy and transaction safety. These threats relevant to e-commerce systems and based on vulnerabilities elicited from the assets of the e-commerce system were analysed using a STRIDE approach throughout Chapter 4 of this research work. The resulting risks were also analysed in this chapter, outlining its impact on the e-commerce system.

The vulnerabilities of assets in an e-commerce system was discussed in section 4.1 based on assets discovered in Chapter 3 thereby proving an answer to this question. The STRIDE method as illustrated in section 4.2 was used to identify security threats to an e-commerce system. Threat identification as seen in this research work is a significant activity for continuous risk management in an e-commerce system. Security threats and its attack patterns change over time even when system assets do not change, and new ways of attacking assets are being discovered. Keeping up with all this demands proper and swift threat identification.

The impacts of security threats that result in risks can be illustrated in section 4.4. These impacts can be emulated by how security criteria are negated by the threat resulting in the loss of confidentiality, integrity or availability of the business assets. However, besides the direct negation of the security criteria of business assets, other impacts are seen as secondary in this research work.

Research Question 3: What are the risk treatment procedures in risk management for an e-commerce system?

The risk treatment procedures have been discussed all through Chapters 5 and 6 of this research work. The role of security risk requirements as a definition of the conditions to be fulfilled to ensure a secure system has been discussed in section 5.1 with some illustrations of its application to the Webshop business process in section 5.2. Security risk requirements are also fundamental to countermeasure selection and implementation as demonstrated in sections 5.2, 5.3 and 5.4.

With the understanding that simultaneously fixing all risk is unrealistic, a security risk metric can be estimated following value estimation of risk concepts using the GQM approach as discussed in section 6.2. Risk reduction levels can also be discovered at this stage.

The risk concepts considered in this metric are;

- Business Asset value
- Security Objective (CIA) value
- Threat likelihood value
- Vulnerability value

- Cost of countermeasure value

Also, the use of risk trade-off analysis techniques as illustrated in section 6.3, demonstrates risks of high, medium and low priority.

The above three research questions and answers to the research questions come together in providing an answer to the main research question of this master's thesis –

What procedure can be used to carry out risk management with a focus on evolving threats to e-commerce systems?

A suitable procedure is one that will provide a way to discover threats to an e-commerce system and consistently follow up the risk analysis procedure up until the treatment of the resulting risks. This is done by the combination of a threat modeling method – STRIDE, with the risk management methodology – ISSRM. Here, the ISSRM methodology is complemented with a streamlined introduction of the STRIDE constructs, providing a systematic way to carry out continuous risk management from asset identification up unto the treatment of risk.

8.3 Concluding Remarks

The idea for this research work was guided by a main research question, "*What procedure can be used to carry out risk management with a focus on evolving threats to e-commerce systems?*" Thus, this research work used the ISSRM method and STRIDE approach in the identification of business context and assets for an e-commerce system, threat modelling, and risk analysis as well as the application of risk treatment procedures.

In carrying out security risk management, it can be seen that a meaningful continuous security risk assessments and treatment decisions in e-commerce systems be carried out in an unambiguous and clear manner using business-relevant terms and proffering mutual understanding between IT and business stakeholders. This has been illustrated throughout this research work with the example of an order fulfilment management process for a Webshop case-study. The use of business relatable modelling techniques to illustrate the asset, risk, and risk treatment scenarios demonstrates its usefulness to both IT and business stakeholders in enabling enhanced risk communication between parties involved in the risk management procedure.

It was also noticed that this approach is useful for the stages of the e-commerce system development cycle and following this approach allowed the introduction of new requirements and the improvement of old requirements to the system depending on the phase of development. With the use of risk measurement procedures, risk reduction levels can be estimated and help with risk treatment decisions provided from a trade-off analysis on the resulting risk metric estimations. It can be summarized that this approach to security risk management is a relevant approach towards a continuous security risk management cycle with emphasis on the evolving threats posed on e-commerce systems.

8.4 Proposals for Future Work

In the course of this master thesis, some issues have been identified as a proposal for future works. Briefly, these issues will be introduced and discussions that provide a background for future academic work on these issues will be opened up.

Even as this research work was not implemented on a live e-commerce system, it simulates the behaviour of one in a useful case study illustration based on a survey of e-commerce systems. However, there is room for improvement in this case as the viability of this approach is subjective until otherwise implemented on a live system.

Also, the e-commerce system type discussed here is the business-to-customer type. This, however, is only one of many other e-commerce types, each having its unique assets. Thus an analysis of other e-commerce system types is a useful scope extension for this proposed approach.

9 References

[1] Altuhhova O., Matulevičius R. and Ahmed N., "An Extension of Business Process Model and Notation for Security Risk Management", *International Journal of Information System Modeling and Design*, vol. 4, no. 4, pp. 93-113, 2013.

[2] Bertino E., Martino L.D., Paci F., Squicciarini A.C. Web Services Threats, Vulnerabilities, and Countermeasures. In: *Security for Web Services and Service-Oriented Architectures*. Springer, Berlin, Heidelberg, 2009.

[3] Breach Level Index. "Data Breach Database - Breach Level Index." *2018*. [online] Available at: http://breachlevelindex.com/data-breach-database [Accessed 30 Mar. 2018].

[4] Capec.mitre.org. "CAPEC - CAPEC List Version 2.11." *2018*. [online] Available at: https://capec.mitre.org/data/index.html [Accessed 31 Mar. 2018].

[5] Cwe.mitre.org. CWE -Common Weakness Enumeration. 2018. [online] Available at: http://cwe.mitre.org/index.html [Accessed 3 Apr. 2018].

[6] Dubois E., Heymans P., Mayer N., Matulevičius R., A Systematic Approach to Define the Domain of Information System Security Risk Management. In: *Intentional Perspectives on Information Systems Engineering*. pp. 289-306. Springer, 2010.

[7] Easterbrook S., *Fundamentals of Requirements Engineering*. 2004.

[8] Firesmith D., "Common Concepts Underlying Safety Security and Survivability Engineering". *Acquisition Support Program.* Technical Note CMU/SEI-2003-TN-033, 2003.

[9] Firesmith D., "Engineering Security Requirements". *Journal of Object Technology* 2(1), 53–68, 2003.

[10] Fortune. Consumers Are Now Doing Most of Their Shopping Online. 2018 [online] Available at: http://fortune.com/2016/06/08/online-shopping-increases/ [Accessed 5 Mar. 2018].

[11] Gaithersburg, National Institute of Standards and Technology. "Managing Information Security Risk: Organization, Mission, and Information System View*" NIST: NIST Special Publication 800-39.*, 2011.

[12] Gaithersburg. National Institute of Standards and Technology. "Guide for Conducting Risk Assessments". *NIST: NIST Special Publication 800-30*, 2012.

[13] Gaithersburg. National Institute of Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Special Publication 800-53 Revision 4.* [online] Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf [Accessed 19 Mar. 2018].

[14] Greenstein M., and Vasarhelyi M., *Electronic commerce*. Boston: McGraw-Hill/Irwin, 2004.

[15] Hevner A., March S., Park J., Ram S.: Design Science In Information Systems Research. MIS Quaterly Research Essay, March 2004.

[16] IEEE Conference Publication, "The security risk analysis of E-commerce and measure research", Ieeexplore.ieee.org, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/5496496/. [Accessed: 05- Dec- 2017].

[17] Isaca.org. The Risk IT Framework Excerpt. 2009 [online] Available at: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf [Accessed 14 Mar. 2018].

[18] Iso.org. 2018 [Online] Available at: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en:term:3.1 [Accessed 5 Mar. 2018].

[19] ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management. 2018. [online] Iso.org. Available at: https://www.iso.org/standard/56742.html [Accessed 5 Mar. 2018].

[20] Matulevičius R., *Fundamentals of Secure System Modelling*. Cham: Springer, 2017.

[21] Mayer N., Dubois E., Matulevicius R., and Heymans P. *Towards a Measurement Framework for Security Risk Management*, 2018. [ebook] Available at: http://ceur-ws.org/Vol-413/paper17.pdf [Accessed 27 Feb. 2018].

[22] Msdn.microsoft.com, "The STRIDE Threat Model", 2018. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx. [Accessed: 04-Mar- 2018].

[23] Msdn.microsoft.com. "Threats and Countermeasures", 2018. [Online]. Available: https://msdn.microsoft.com/en-us/library/ff648641.aspx. [Accessed: 20- Apr- 2018].

[24] Muckin M., and Fitch S., A Threat-Driven Approach to Cybersecurity. *Lockheed Martin Corporation*, 2018.

[25] National Institute of Standards and Technology. National vulnerability database https://nvd.nist.gov. [Accessed: 05- Dec- 2017].

[26] Owasp.org. "OWASP Application Security Verification Standard - OWASP." *(2018).* [online] Available at: https://www.owasp.org/index.php/OWASP_Application_Security_Verification_Standard#15.7 [Accessed 1 Apr. 2018].

[27] Owasp.org. "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks", 2017. [Online]. Available: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. [Accessed: 05- Dec- 2017].

[28] Overton A., "Ecommerce Shipping: Strategies, Solutions & Best Practices [for 2017]", The BigCommerce Blog, 2017. [Online]. Available: https://www.bigcommerce.com/blog/ecommerce-shipping/. [Accessed: 05- Dec-2017].

[29] PCI Data Security Standard (PCI DSS). Information Supplement: Best Practices for Securing E-commerce. 2017. [ebook] Available at: https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf [Accessed 12 Mar. 2018].

[30] Ramona E., and Cristina A., “Security Risk Management - Approaches and Methodology”. [ebook] Academy of Economic Studies, Bucharest, Romania: Informatica Economică vol. 15, no. 1/2011, pp.228 - 240. 2018.

[31] Samarütel S., Matulevičius R., Norta A. and Nõukas R., "Securing Airline-Turnaround Processes Using Security Risk-Oriented Patterns", *The Practice of Enterprise Modeling*. Lecture Notes in Business Information Processing, vol 267. Springer, Cham PoEM 2016.

[32] Schneier.com. Academic: Attack Trees - Schneier on Security. [online] Available at: https://www.schneier.com/academic/archives/1999/12/attack_trees.html [Accessed 12 Mar. 2018].

[33] Shostack A., *Threat modeling: Designing for Security*. Indianapolis: Wiley, 2014.

[34] The Green Sheet. “The Worldwide Fraud Web Exposed,” April 22, 2010.

[35] Tsipenyuk K., Chess B. and McGraw G., "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors", *IEEE Security and Privacy Magazine*, vol. 3, no. 6, pp. 81-84, 2005.

[36] Tsoumas B., Papagiannakopoulos P., Dritsas S., Gritzalis D., Security-by-ontology: A Knowledge-centric Approach. In: Boston, S. (ed.) *Security and Privacy in Dynamic Environments*. pp. 99–110 (2006)

[37] Turban E., Volonino L., McLean E., and Wetherbe J., Information Technology for Management: Transforming Organisations in the Digital Economy, the seventh International student edition. Hoboken, NJ: Wiley, 2010.

[38] Udokwu C., Norta A. And Matulevicius R., "Analysis of digital security threats in aviation sector", Master's Thesis, Tallinn university of technology, 2017.

[39] US-CERT, Vulnerability notes database. [online] Available at: http://www. kb.cert.org/vuls/. [Accessed: 05- Dec- 2017].

[40] Xin T. and Xiaofang B., “Online Banking Security Analysis based on STRIDE Threat Model” International Journal of Security and Its Applications, vol.8, No.2, pp. 271-282, 2014.

[41] Yanyan W., “Research on e-commerce Security based on Risk Management Perspective”, International Journal of Security and Its Applications, vol.8, No.3, pp. 153-162, 2014.

Appendix

I License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Affia, Abasi-amefon Obot**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Security Risk Management of E-commerce Systems,

(title of thesis)

supervised by Raimundas Matulevičius,

(supervisor's name)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **21.05.2018**