

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technology

Department of Software Science

Chibuzor Joseph Udokwu

ANALYSIS OF DIGITAL SECURITY THREATS IN AVIATION SECTOR

Master's Thesis

Supervisor: Alex Norta
(Associate Prof.)

Supervisor: Raimundas
Matulevicius
(Associate Prof.)

Tallinn 2017

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Chibuzor Joseph Udokwu

17.01.2017

Acknowledgement

I want to appreciate all the persons that made significant contributions towards the successful completion of my master thesis. I am grateful to my academic supervisors Alex Norta and Raimundas Matulevicius for their patience and guidance throughout the course of this master thesis. The opportunity to work with them as my supervisors exposed me to scientific thinking that is required to become a good researcher.

I am also grateful to the Jeppesen cybersecurity team for the opportunity to carry out this project. Most importantly, I am grateful to Katarzyana for her support and constructive feedback especially in the area of airline turnaround operations and simulations carried out in this work.

Abstract

Enterprises engage in outsourcing and collaboration activities in order to complete tasks which are not part of their core business operations. Collaboration between enterprises and service providers are usually supported by IT systems in the process of communicating and exchanging service requirements. This has resulted in security concerns because information that contains crucial aspects of business is exchanged in the process.

This thesis proposes to analyse digital security threats in airline operations as a result of collaboration between enterprises using airline turnaround as a case study. The background of this thesis is collaboration between Tallinn University of Technology and Jeppesen airline and maritime services. As a result, workflows in airlines day of operations are examined to determine security issues caused by collaboration between airlines and service providers in aviation sector.

The scientific approach in solving this problem is composed of three steps in applying information risk management framework for the analysis. The first step is to identify assets that are involved in the collaboration. The second step is to determine the risks by exploring the risk components of the identified assets. The final step is the application of security requirements and controls to mitigate the risks on these assets. Evaluation is performed to establish how security requirements and controls reduced the risks.

The final part of this thesis is a simulation demonstrating the risk analysed as a sociotechnical setup. This is achieved by using a viewpoint framework to model and describe an example of a cyber-attack resulting from one of the risks analysed.

This thesis is written in English language and is 110 pages long, including 7 chapters, 20 figures and 28 tables.

Annotatsioon

[Thesis title in Estonian]

[Tekst]

Lõputöö on kirjutatud [mis keeles] keeles ning sisaldab teksti [lehekülgede arv] leheküljel, [peatükkide arv] peatükki, [jooniste arv] joonist, [tabelite arv] tabelit.

List of abbreviations and terms

Abbreviation	Description
ACARS	Aircraft Communications Addressing and Reporting System
ADS-B	Automatic Dependent Surveillance –Broadcast
AOM	Agent Oriented Modelling
ATC	Air Traffic Control
CG	Centre of Gravity
CIS	Centre for Internet Security
CCTA	Central Computer and Telecommunications Agency
CORAS	Risk Assessment of Security Critical Systems
CRAMM	CCTA Risk Analysis and Management Method
DOO	Day of Operation
DNS	Domain Name Server
FMS	Flight Management Systems
ICT	Information Communication Technology
IT	Information Technology
ISSRM	Information security risk management
IS	Information System
ISO	International Standard Organization
MAS	Multi-Agent System
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation

PKI	Public key infrastructure
RQ	Research Question
SMTP	Simple Mail Transfer Protocol
SaaS	Software as a Service
VE	Virtual Enterprise
TLS	Transport Layer Security

Table of contents

1.	Introduction	13
1.1	Goal of the thesis.....	13
1.2	Literature Review.....	14
1.2.1	Digital security issues in the Aviation.....	14
1.2.2	Outsourcing, collaboration and security challenges.....	16
1.3	Research Method.....	18
1.3.1	Design Science.....	18
1.4	Research Questions.....	20
2.	Background.....	23
2.1	Previous work.....	23
2.1.1	Service brokering agreement for airline.....	23
2.1.2	Agent oriented modeling and multi-agent systems.....	24
2.2	Risk Management.....	26
2.2.1	Risk Management Frameworks.....	26
2.2.2	Information security risk Management frameworks.....	27
2.2.2 .1	ISO/IEC 27005 Risk Management method.....	28
2.2.2 .2	Octave Method.....	30
2.2.2 .3	ISSRM Domain Model.....	31
2.2.2 .4	GQM Framework.....	34
3.	Identification of assets in enterprise collaboration.....	36
3.1	Airline day of operation.....	36
3.1.1	Flight preparation.....	37
3.1.2	Take off.....	37
3.1.3	Turnaround.....	37
3.2	Assets in airline turnaround.....	40
3.2.1	Passenger management process.....	40
3.2.1.1	Checked-in passenger information.....	40
3.2.1.2	Luggage information.....	42
3.2.2	Ground operations.....	43
3.2.2.2	Fuelslip.....	43
3.2.2.2	Cargo assignment.....	44

3.3	Conclusion.....	45
4.	Risk analysis of assets in turnaround	47
4.1	Passenger management risk analysis.....	48
4.1.1	Checked-in passenger risk analysis.....	48
4.1.2	Luggage information risk analysis.....	51
4.2	Ground operations risk analysis.....	53
4.2.1	Fuelslip risk analysis.....	54
4.2.2	Cargo assignment risk analysis.....	56
4.3	Conclusion	59
5.	Risk Treatment and Evaluation.....	61
5.1	Risk treatment.....	61
5.1.1	Checked-in passenger information risk treatment.....	62
5.1.2	Luggage information risk treatment.....	63
5.1.3	Fuelslip risk treatment.....	64
5.1.4	Cargo assignment risk treatment.....	66
5.2	Evaluation of risk	67
5.2.1	Maximizing risk reduction.....	67
5.2.2	Risks Metrics and calculations	67
5.2.3	Risk1 reduction metrics	68
5.2.4	Risk2 reduction metrics	69
5.2.5	Risk3 reduction metrics	70
5.2.6	Risk4 reduction metrics	72
5.2.7	Risk5 reduction metrics	73
5.2.8	Risk6 reduction metrics	74
5.2.9	Risk7 reduction metrics	75
5.2.10	Risk8 reduction metrics	76
5.3	Analysis of risk metrics.....	77
5.4	Conclusion	81
6.	Risk Simulation.....	82
6.1	Description of risk.....	82
6.1.1	Interception of airline fuelslip.....	82
6.1.1.1	Mailing list attack.....	83
6.1.1.2	DNS poisoning attack.....	83
6.2	Platform independent simulation models.....	84

6.2.1	Goal model.....	84
6.2.2	Role model.....	86
6.2.3	Agent model.....	86
6.2.4	Interaction model.....	87
6.2.5	Knowledge model.....	88
6.2.6	Behavioural model.....	89
6.3	Anylogic Based Simulation.....	91
6.3.1	Definition of Symbols.....	91
6.3.2	Airline Refuel Attack Simulation	92
6.3.3	Analyses of Simulation Result	94
6.4	Conclusion	96
7.	Conclusion.....	97
7.1	General conclusions.....	97
7.2	Answer to research questions.....	97
7.3	Future works.....	103
	References	106
	Appendix	110

List of figures

Figure1. Design-science research framework [16].....	19
Figure2. Information security risk management process [41].....	29
Figure 3: OCTAVE Information Risk Management Framework [25].....	30
Figure 4: ISSRM Domain Model [24].....	33
Figure 5: Example of GQM Model [26].....	34
Figure 6: GQM risk reduction maximizing goal [24].....	35
Figure 7: GQM Risk Treatment minimizing goal [24].....	35
Figure8. Airline turnaround phase of day of operation [43].....	39
Figure9: Graph1.....	79
Figure 10: Graph2.....	79
Figure 11: Graph3.....	80
Figure 12: Risk simulation goal model.....	85
Figure13. Risk simulation Agent Model.....	87
Figure14. Risk interaction model.....	87
Figure15. Risk simulation knowledge model.....	88
Figure16. Risk behavioural model.....	89
Figure 17. Airline Refuel Attack before Application of Security Controls.....	92
Figure 18. After Application of Security Controls.....	93
Figure 19. Chart of Airline Refuelling before Application of Security Controls.....	110
Figure 20. Chart of Airline Refuelling After Application of Security Controls.....	110

List of tables

Table1. The viewpoint framework [30].....	25
Table2. ISSRM Domain Model Concepts [24].....	32
Table3 Checked-in passenger information asset Identification table.....	41
Table4. Luggage information asset identification table.....	42
Table5. Fuelslip asset Identification table.....	44
Table6. Cargo assignment asset identification.....	45
Table7. Checked-in passenger information risk analysis.....	48
Table8. Luggage information risk analysis.....	51
Table9. Fuelslip risk analysis.....	54
Table10. Cargo assignment risk analysis.....	57
Table11. Checked-in passenger information risk treatment.....	62
Table12. Luggage informarion risk treatment.....	63
Table13. Fuelslip risk treatment.....	64
Table14. Cargo assignment risk treatment.....	66
Table15. Risk 1 reduction metrics.....	68
Table16. Risk 2 reduction metrics.....	69
Table17. Risk 3 reduction metrics.....	70
Table18. Risk 4 reduction metrics.....	72
Table19. Risk 5 reduction metrics.....	73
Table 20. Risk 6 reduction metrics.....	74
Table 21. Risk 7 reduction metrics.....	75
Table 22. Risk 8 reduction metrics.....	76
Table 24: Risk Priority Table	78
Table 25: Risk simulation role model.....	86
Table 26: Description of Anylogic Process Modelling Blocks [44].....	91
Table 27: Airline refuelling simulation result.....	94
Table28: Effect of attack on Airline resources.....	95

1 INTRODUCTION

The civil aviation industry plays a crucial role in the economy of any nation. The tremendous growth in the aviation sector in the past decades has resulted in increase of outsourcing activities. The competition in the sector and the need to make profit has necessitated airline operators to outsource some of their operations that are not part of their core competences [32].

As airlines and service providers engage in collaborations, assets are generated and exchanged in the process. The collaboration process and assets generated in the process are supported by IT systems that reside both within the organizations and the service providers. These assets contain crucial information such as business secrets, strategy, rules etc. By exchanging such information with third parties, airlines are exposed to security threats that they don't have direct control over.

There is need to analyze and understand the importance of each asset identified and the role it plays in a collaboration process. The analysis is also necessary in order to comprehend the security threats on the assets identified and impact of such threats on the enterprise.

1.1 Goal of the thesis

This thesis focuses on analyzing threats that are caused as a result of collaboration and outsourcing activities between airlines and service providers. The aim of this work is to apply a security framework for analyzing and managing risks generated in enterprise collaborations using the aviation sector as a case study. As airlines continue to use computer systems to support collaboration with services providers, this work seeks to prepare airlines for secure virtual collaborations between airlines and service providers that are supported by cloud-computing infrastructures. While migration to cloud supported collaboration presents great benefit to the airlines, the security risk which they present cannot be ignored [33]. By applying an information system risk management framework, we can analyze, evaluate and manage security risks resulting from enterprise collaboration.

1.2 Literature Review

The literature review for this work is divided in two sections, the first section discusses current security threats in the aviation industry and how collaborations between enterprises could lead to security concerns. The last section in the literature review discusses outsourcing, collaboration and virtual enterprises as it relates with the aviation industry.

Section 1.2.1 starts by reviewing literature discussing the overview of current digital security issues in the aviation sector. Section 1.2.2 describes relationship between outsourcing and collaboration and the role they play in the aviation sector. The section further discusses security threats that are resulted from collaboration between enterprises.

1.2.1 Digital security issues in Aviation

The digital maturity in the aviation sector has increased rapidly which is a result of heavy dependence of this sector in IT systems and tools as airlines are advanced users of ICTs and a good number of airline functions rely heavily on Information systems and have invested heavily in computer systems since 1950s [1]. As a result of airlines reliance on IT systems, the cyber security attacks on the aviation sector has increased rapidly. The 2013 annual report released by Centre for Internet Security (CIS) shows that 75 airports in the US have witnessed cyber-attacks and the systems in two of the airports have been successfully compromised [2].

The first cyber security attack that resulted in a ripple effect on the aviation sector occurred on 10 March 1997. A teen hacker crashed Bell Atlantic telephone company affecting the telephone system at Worcester Airport thereby grounding the airport for about 6 hours. The telephone and radio communication systems used by the control tower, fire department and weather service were all knocked-out [3]. While recent security incidents in the aviation sector are usually attributed to human error or computer glitch¹ therefore it's difficult to attribute such events which are truly cyber

¹ In July 2015, United Airline attributed an incident which grounded the airline over an hour and affected about 4,900 flights as network connectivity issue
<http://money.cnn.com/2015/07/08/news/companies/united-flights-grounded-computer/?iid=EL>

security incidents to nation states, terrorists, organized crime, or hackers [4]. However, researchers have severally demonstrated how easy it is to hack digital systems that support aviation and airline industry.

Cyber-attacks can be carried out on Automatic Dependent Surveillance -Broadcast (ADS-B) systems. A security researcher demonstrates how practical attacks can be carried out on ADS-B protocols and devices. The main goal of the ADS-B is to independently determine the location of an aircraft and thereby increase safety of air traffic. The attack was carried in a controlled environment using a commercial off-the-shelf (COTS) transmitter. A software defined radio transmitter is used in transmitting attacker's messages, encoding was achieved using special software [5]. The researcher used commercial COTS to show a successful reception of attacker's message. The aim of the hack was to demonstrate how ADS-B systems in the aircraft can easily be spoofed.

A security researcher shows how flight control can be hijacked by using COTS devices and specially designed software. In a YouTube video¹ the researcher shows the vulnerabilities present in ADS-B, Aircraft Communications Addressing and Reporting System (ACARS), Flight Management Systems (FMS). The hack demonstrates how the vulnerabilities present in these systems could be exploited, leading to a successful hijack of flight control [6].

The attacks described above focus on attacking into the avionics via the entertainment network, hacking ADS-B, hacking engine systems, hacking ACARS and other ATC supporting systems. Though it has not been proven that hacking of these systems could lead to an air crash as manual validation exists for most of these systems, continuous attacks in a distributed fashion on ATC systems can increase the chance of human error [7]. Investigation by the French Bureau d'Enquetes et d'Analyses has shown that misleading speed indications from wind speed sensors as well bad weather conditions

¹ A YouTube video <https://www.youtube.com/watch?v=wk1jIKQvMx8> of Hitb Security Conference 2013

played a role in the crash of Air France flight 447 [8]. However, unconventional cyber-attack can be carried out in the aviation sector by exploiting the weaknesses that are present in the current collaboration and outsourcing setup in the aviation industry. Some of the attacks and weaknesses present in the collaboration setup are explained in the section 1.2.2 below.

1.2.2 Outsourcing and virtual enterprise collaborations and security challenges

Outsourcing and collaborations play a key role in the business operations of airlines in the aviation industry. Competition in the sector and the need to make more profit have been a major driving factor in causing airlines to outsource operations that are not part of their core business processes [29].

The term collaboration can be defined as a process where two or more individuals, groups or enterprises work together to achieve a common goal. Enterprise collaboration is therefore defined as the means by which people within different business silos or geographical locations work together using the Internet as a collaboration medium and by so doing establish a collaborative network [9]. Completing an outsourced project can be an example of a common goal that brings two organizations together. The client provides details and specifications as regards an outsourced task, while the service provider communicates and delivers the task through the same channel. Therefore, we can restate collaboration as the cooperation between the airlines and service providers in the process of completing the outsourced tasks. From the definition of enterprise collaboration, it can be deduced that the collaboration operations are supported by IT systems and computer networks. In the process of collaboration, information that contain data about critical aspects of a business are exchanged between the computer networks and IT systems of involved parties. This creates unique organizational challenges in terms of securing precious corporate assets and managing corporate risk [10].

With the emergence of cloud computing, organizations have adopted a new way of collaboration that is often referred to as virtual enterprise collaborations. A virtual enterprise (VE) is a temporary alliance of enterprises that come together to share skills or core competencies and resources in order to better respond to business opportunities,

and this type of cooperation is supported by computer networks [11]. Collaborations like these emphasize the temporal nature of the cooperation and the clusters of organizations involved in resource sharing. This type of collaboration process is supported by a cloud computing infrastructure since conventional computer networks cannot achieve this type of collaborations. Cloud computing is defined as parallel and distributed systems comprising of a collection of different inter-connected and also virtualized computers presented as one or more unified computing resources [12]. This definition reaffirms our description of how cloud computing supports temporal alliance between a cluster of organizations in sharing resources.

The aviation sector is not left out in virtual business collaborations in modern enterprises. The examples below describe some Software as a Service (SaaS) virtual enterprise collaborations in the aviation sector.

Sabre AirCentre Enterprise¹ is a SaaS Cloud solution that helps airlines in the delivery of flight operations, crew management, airport operations and maintenance planning, while allowing the enterprise to have complete control.

SchedulAir² is another example of SaaS that provides Flight Management solutions from fleet planning to fleet assignment and crew pairing.

More recently in modern aircrafts, a new form of collaboration exists in ground maintenance systems between airline operators and service providers. An example is shown in Honeywell aviation systems.

Honeywell's Onboard Maintenance³ Systems provides a model-based diagnostic approach. The primary goal of the software is to monitor the health of the aircraft and diagnose any issues quickly and accurately [13].

¹ Link to Sabre AirCentre site: http://www.sabreairlinesolutions.com/home/software_solutions/enterprise_operations/

² Link to SchedulAir site: <http://www.decisal.com/solutions/management/>

³ Link to Honeywell site: <https://aerospace.honeywell.com/products/information-and-maintenancemanagement/onboard-maintenance-systems>

These new form of collaboration presents additional security issues in the aviation industry. For airlines using SaaS cloud solutions, issues such as data loss, data breaches, and denial of service could lead to flight delays or outright cancellations of flights. Also for the connected ground maintenance system, an attacker can identify security issues with an aircraft, run an exploit such as resetting the code without repair being carried out and thus, creating potentially an unsafe aircraft [14].

Other security challenges that are introduced to the organization as a result of cloud-computing are increase in the attack surface due to system complexity, loss of control over resources and data due to asset migration, threats that target exposed interfaces due to data storage in public domains, data privacy concerns [15].

These security threats pose a serious challenge to airlines and the aviation industry in delivering safe flights. Therefore, there is a need to apply a risk management framework to identify, analyze and mitigate security threats that are posed in enterprise collaborations. We consider the aviation sector as a rich and suitable case study for this research.

1.3 Research Methodology

A rigorous research method which is design-science is applied in carrying out this research. Design-science is a research framework that creates and evaluates IT artifacts intended to solve identified organizational problems [16]. This is in line with the goal of this master thesis, which is to apply a risk management framework in securing cross-organizational collaboration in the aviation sector.

1.3.1 Design Science Research

Design-science research method provides a framework for creating new theories and artifacts that could be constructs, models, methods, and instantiations. Design-science research is made of three pillars: environment, information system research and knowledge base¹. The environment represents the people and technology that make up an organization. While the knowledge base represents previous knowledge foundations such as theories, methods, models, technique, measures, etc. Design-science helps

¹ A brief description of the diagram - *Information Systems Research Framework* in Hevner et al./Design Science in IS Research. Pg. 80

organizations to address their business needs by conducting research that are relevant to the problems of the organizations. The research is also conducted rigorously by applying knowledge from the knowledge base to develop new artifacts and also to evaluate such artifacts [17].

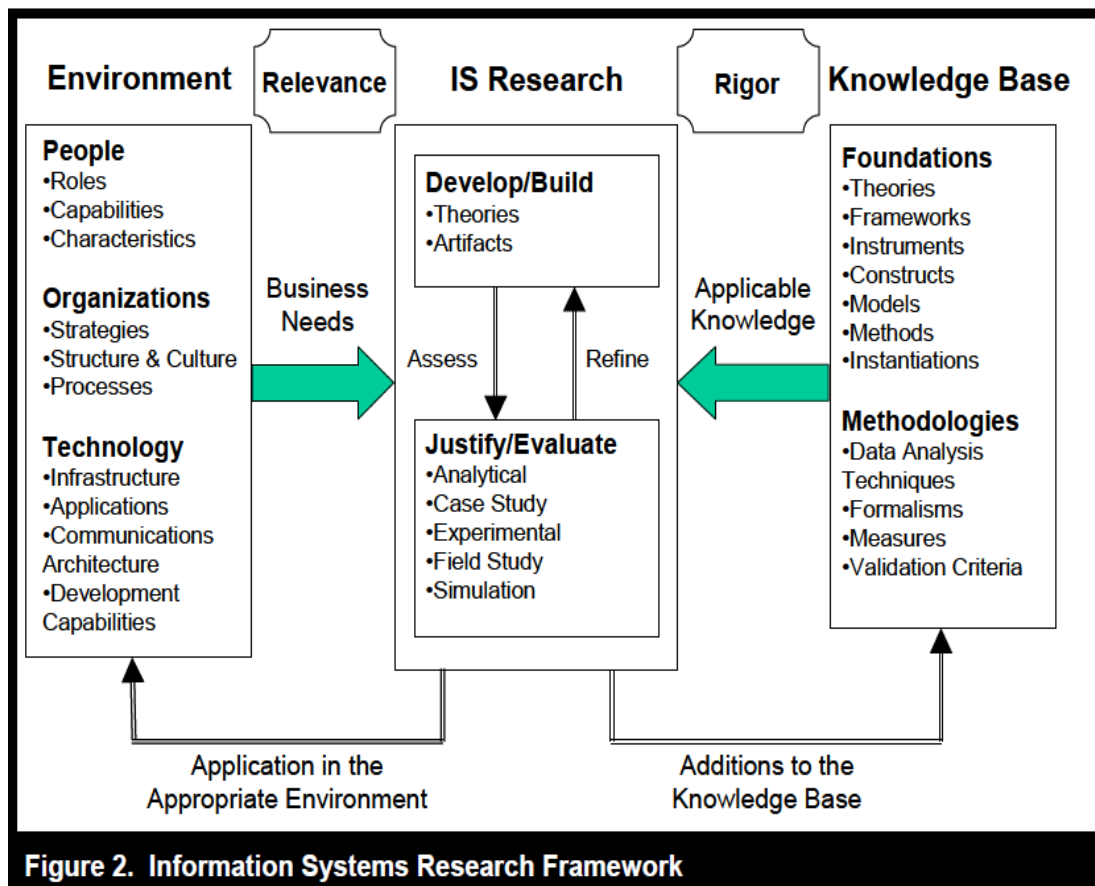


Figure 1 - Design-science research framework for the domain of information systems [16]

The following describes how the research is conducted according to the guidelines of the design-science framework:

Design as an Artifact: The end product of this research work is a security framework for airline turnaround systems. The answers from the questions are used to create security control and requirement models for virtual business collaborations in the aviation industry.

Problem Relevance: The current setup of enterprise collaborations between enterprises lacks security to protect critical business and IT assets. The objective

in this research work is to apply risk oriented patterns to enterprise business processes in order to generate a new security requirement controls for VE-collaborations.

Research Contribution: this thesis contributes to the research society by applying domain model for information risk management in analyzing security threats in enterprise collaborations in aviation industry.

Design Evaluation: the product of this research work, a security framework for airline turnaround systems will be subjected to evaluation by domain experts in the industry. Some of the concepts used in this research such as VE concepts and risk management frameworks have been demonstrated by academic researchers - Alex Norta, PHD and Raimundas Matulevičius, PHD.

Design as a Rigor: In order to secure business assets enterprise collaborations, various data will be analyzed in order to determine which assets are affected in the collaborations. And also, various security requirement patterns will be used to setup a secured business process for VE-collaborations.

Communication of research: this thesis is written for thesis level as a requirement for completion of master's program in e-Governance technologies and services. The analysis made in thesis will be useful to both technical and non-technical audiences such as business analysts, enterprise collaboration experts, cybersecurity experts etc.

1.4 Research Questions

Because of the absence of a detailed framework for analyzing digital security threats in cross-organization collaborations, we propose the following main research questions:

How to analyze security threats in virtual enterprise collaborations?

For establishing a separation of concerns, we break up the main research question into three sequential topics -

- Identification of assets in airline/service-provider collaborations in airline's turnaround workflow.
- Risk analysis of assets in turnaround workflow
- Application of security controls and risk evaluations

The first topic that is the identification of assets airline/service-provider collaborations is discussed in chapter three of this thesis. The second topic - risk analysis of assets in airline turnaround workflow is discussed in chapter four. The final topic - application of security controls, and risk evaluations is discussed in chapter five.

Identification of assets in airline/service-provider collaborations results in the following research question and two sub-questions -

RQ1: How to identify relevant assets in enterprise collaborations that need to be secured?

In order to answer this question, the following what questions are necessary: ·

What IT Systems are involved in these collaborations?

What information is exchanged between collaborating systems?

These two questions help to identify important resources and also the shared data between collaborating systems. By identifying these collaborating systems and relationship dependencies that exist; it must be possible to understand what information is stored and what data is exchanged between collaborating systems. Analyzing strategic relationships helps to understand the impact and extent of threats, and the effectiveness of mitigating measures [18].

Risk analysis of assets in turnaround workflow results in the following research question and four what questions -

RQ2: How do security risks threaten collaboration systems?

The following questions will be used to answer research question 2:

What are the threat agents?

What are vulnerabilities?

What are attack methods?

What are the risk impacts?

These questions are necessary because each of the assets identified in RQ1 possess different kinds of weaknesses and risks for aviation operations and therefore, the need arises to identify such weaknesses and risk impacts. Understanding the impact risks as a result of these threats helps an organization to focus on threats that have higher impacts on core goals. In the case of aviation the core goal is to deliver safe flights and therefore focus will be on threats that have high impact on safety of flights. The major

responsibility of the security analyst is to identify security risks that potentially are characterized by threats, vulnerabilities and risk impact [18].

Application of security controls and risk evaluations results in the following research question and three what questions -

RQ3: How to mitigate security risks in enterprise collaborations?

The following questions are necessary in order to answer RQ3:

What are the security requirements?

What are the security controls that implement the security requirements?

What degree of security is achieved with implementing the security controls?

These questions will help us understand how to tackle the problems identified in RQ3.

In this case, we look at security-requirement controls that we can employ to solve these challenges. To mitigate the risks, the security pattern introduces a security requirement filter for the incoming data [18]. Since there is no perfect security, the answers from the questions give the level of security that is achieved by implementing the risk requirement controls.

2 Background

The goal of this chapter is to introduce previous works leading to this master thesis and also presents frameworks and methods which are used in the rest of the chapters of this work. The background of this master thesis is divided into two sections. The first section summarizes previous work done in [21] and also presents the viewpoint framework agent based modeling. The viewpoint framework is applied in the simulation part of this master thesis. The second section discusses risk analysis risk analysis frameworks and also the Domain Model for Information System Security Risk Management (ISSRM). The methods described in the ISSRM Domain Model are used in the analysis that is carried out in this work.

2.1 Previous works

This master thesis is a continuation master thesis work - “Service Brokering Environment for an Airline” that demonstrates how an organization can transform its business processes to enable enterprise collaboration [21]. The second part of this subsection discusses methods in viewpoint framework.

2.1.1 Service brokering environment for airline

The master thesis in [19] describes how workflows in the aviation industry could be transformed to enable virtual enterprise collaboration with third party service providers. The tasks performed in the thesis work can be outlined as follows -

- Normalization of airlines workflows

The author used choreography business process models¹ to describe details of day to day operations of a typical airline. The day to day operations described represent the workflows of an airline. The workflows include the following: short-term planning phase workflow, day of operation shift phase workflows, day of operation flight plan preparation phase workflows, day of operation flight plan calculation workflows, and day of operation actual flight workflows.

¹ Choreography modelling is fundamentally designed to support B2B collaborations in a single business process perspective (Ryan K.L., 2009)

- Refining of airlines business process model:

The author improved and elaborated the normalized workflows to realize a real life scenario. The new processes are represented by three day of operation activities of an airline and they are: flight preparation day of operation, turnaround day of operation and takeoff.

- Reconfiguration of airlines digital architecture demonstrating collaboration mechanism:

The author demonstrates how the refined processes can be transformed for easy and effective cloud based collaboration using a conceptual e-sourcing mechanism. This, the author described, can be achieved by breaking down the airline's work processes into public view and private view. The internal view represents the internal work processes of the organization while the public view outlines the specifications and expectations of an organization for an outsourced work process. To demonstrate this, the author used a case study of airline refueling process to show bidding and coordination parts of the collaboration mechanism.

The case study analysis performed in this master thesis is based on the normalized airline turnaround workflow described in [21]. The decision to use the airline turnaround workflow is because the turnaround phase provides more opportunities for collaborations between the airline and service providers. The activities involved in this phase are resource intensive and are not part of the core competence of the airlines.

2.1.2 Agent Oriented Modeling and Multi-agent System

Multi-Agent System (M.A.S) describes a complex system consisting of more than one agent and are able to interact within an environment. A M.A.S is defined as a system in which multiple entities, called agents; interact in a shared environment, aimed to achieve some individual or collective goals [31]. An agent is an entity that is capable of sensing its environment and respond accordingly. In some cases, agents within the system comprises of both human and non-human agents. Such multiagent system is referred to as socio-technical system. A sociotechnical system can loosely be described as a system which is made up of both social aspects (human agents) and technical aspects (non-human agents) [30].The simulation that will be performed in the later

chapter of this master thesis illustrates a sociotechnical setup because it involves human agents interacting with non-human agents in the same environment.

The agent oriented modeling (AOM) provides a method for modeling and simulating a multi-agent system. Agent based modeling techniques are applied in development of agent computer based simulations; from conceptual phase to deployment phase. The Viewpoint Framework is an AOM method that describes a modeling method for distributed systems which is based on three abstraction layers: conceptual layer, design layer and deployment layer [30].

Table 1. The viewpoint framework [30]

Viewpoint models	Viewpoint aspect		
Abstraction layer	Interaction	Information	Behaviour
Conceptual domain modelling	Role model and organization model	Domain model	Goal model
Platform- independent computational design	Agent model, acquaintance model, interaction models	Knowledge model	Behaviour models
Platform-specific design and implementation	Agent interaction specifications	UML class diagram	Agent messaging diagram

The abstraction layers are represented by three viewpoint aspects. The first two abstraction layers: conceptual models and design models layers are platform independent, while the last layer outlines a platform specific design model. Our goal is to use the viewpoint to model a platform independent simulation of the risk analysis performed in this master thesis, and therefore our focus will be on the first abstraction layers of the viewpoint framework.

The following briefly describe each of the models identified in viewpoint framework as shown in the Table1.

Goal models: The goal model describes a set of objectives in hierarchical order which is to be achieved by an agent. The goals are divided into functional and

non-functional goals. The non-functional goals are also called quality goal because they describe how the functional goal is to be achieved.

Role model: the role model outlines all the responsibilities an agent needs to fulfill in order to achieve its set of goals. It also contains the constraint and limitations of the agent.

Agent Model: this model shows the transformation of abstract construct (role) to design constructs (agent types) and also shows the interaction pathways between agents.

Knowledge models: the knowledge model describes the ontology of communication between agents. This is necessary in order for agents to pass clear information to other agents.

Behaviour model: the behaviour model illustrates interaction taking place between an agent and other agents interacting with it. It also describes the rule governing such interactions.

2.2 Risk Management

In this section we introduce risk management and risk management frameworks. Also, we describe in details the frameworks and methods we will employ in our analysis of airline turnaround process. This section is further divided into two subsections, 2.2.1 and 2.2.2. Section 2.2.1 discusses risk management frameworks while section 2.2.2 presents ISSRM domain model.

2.2.1 Risk Management Frameworks

International Standard Organization defined information security risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization [20]. And according to Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), information security risk can be broken into four major components: asset, threat, vulnerability, and impact [21]. Therefore in order to understand and manage information security risks, all these four components must be accounted for. These four risks components are described as follows-

Asset: Assets are defined as anything that has a value for the organization and that is central to the achievement of business goals [22]. Though there are many literature

classifications of asset, however we concentrate our discussion to the definitions of asset in terms of business and information system (IS) assets. A Business Asset is defined as valuable aspects of a business, such as workflow, rules, components, transaction, people, strategy, laws, etc. [22]. From this definition, it can be deduced that most aspects of an enterprise that plays a role in achieving its goals can be classified as business assets. The IS assets technically supports the business asset in achieving enterprise goals and objectives. IS assets are those IT resources or other components that are part of the IS, linked to the business assets [24]. For instance, IS assets are information system components like computers, software, databases, business process etc. The value of each asset in the organization differs, and therefore risk resulting from threats on each asset differs too.

Threat: A threat is an indication of a potential undesirable event.

Vulnerability: A weakness in the system which can be exploited.

Impact: negative effect or consequence of a potential undesirable event.

2.2.2 Information Security Risk Management frameworks

Information security risk management is an ongoing process of identifying and addressing information security risks [25]. It includes an organized approach in identifying, describing and managing IS risks. Several methods and frameworks have been developed to help organizations in managing information security related risks. Some of the approaches for information security risk management are listed as follows – ISO risk management method, CORAS framework, CRAMM, OCTAVE etc.

ISO/IEC 27005 is an information technology risk management techniques. It provides guidelines on how organizations can manage their information security related risks [37]. CRAMM (CCTA¹ Risk Analysis and Management Method) is a qualitative risk assessment tool developed in 2001. CRAMM was developed from input from security experts in private and public also providing benchmark suitable for most organizations in risk and contingency management. CRAMM risk assessment toolkit is automated software that manages risk by identifying and valuing assets, performing threat and vulnerability assessment, risk analysis and risk management [38]. CORAS is a model based method for security risk analysis. The CORAS concepts for risk assessment are as

¹ CCTA – Central Computer and Telecommunications Agency

follows – identification of targets for evaluation, risk analysis of targets and treatment of identified risks [39]. The OCTAVE framework is an approach for managing information security risks. OCTAVE uses a three-phase approach in exploring organizational and technological issues, thereby developing a complete picture of information security needs of such organizations [34].

In the subsections below, we describe the following three risk management frameworks - ISO/IEC 27005 Risk Management Method, OCTAVE framework, and ISSRM Domain model. Section 2.3.2.1 discusses the ISO/IEC 27005, in section 2.3.2.2 we introduce and describe briefly OCTAVE framework for IS risk management. Our decision to choose and describe the OCTAVE framework is because some of the risk concepts used in ISSRM Domain model are derived from Octave framework. The concluding part, of this section 2.3.2.3 describes ISSRM Domain Model framework that is used in our analysis and also used in evaluation security controls applied in the analysis.

2.2.2.1 ISO/IEC 27005 Risk Management Method

ISO/IEC 27005 is an information security risk management process that is divided into 3 phases – context establishment, risk assessment and risk treatment. The three phases are repeated in a loop until risks are reduced to an acceptable level [41].

Context establishment: This is the first phase of risk management process. It involves establishment of basic criteria in which the risk management process will be conducted. The following criteria are clearly stated – risk evaluation criteria, impact criteria and risk acceptance criteria.

Risk evaluation criteria: The following points are consider in developing risk evaluation criteria for organizations –Strategic value of business process, criticality of information asset, legal and regulatory requirements, and stakeholders expectations.

Impact criteria: the following are considered in developing impact criteria –level of classification of affected asset, breach of information security, loss financial value, disruption of business, damage of reputation, and legal breaches.

Risk acceptance criteria: is the threshold, or level of risk that is acceptable. The levels are based on points considered in impact criteria of the risk.

Information security risk assessment: The risk analysis phase of the risk management process is broken down into risk analysis and risk evaluation.

Risk analysis: this involves identification of risks by identifying the components that make up the risk. The following risk components are identified in risk analysis – assets, threats, existing controls, vulnerabilities and consequences.

Risk evaluation: this is a method for estimating the levels of risk identified in the previous stage. Two approaches can be used to achieve this, qualitative estimation and quantitative estimation. Qualitative approach estimates the risk as low, medium or high risk. Quantitative approach uses a numerical figure in estimating the value of risk.

Risk treatment: The risks identified in the analysis phase are treated based on the following objectives or risk treatment options – reduction of risk, retention of risk, avoidance of risk, and transfer of risk. Security controls and conditions are applied to achieve any of risk treatment options.

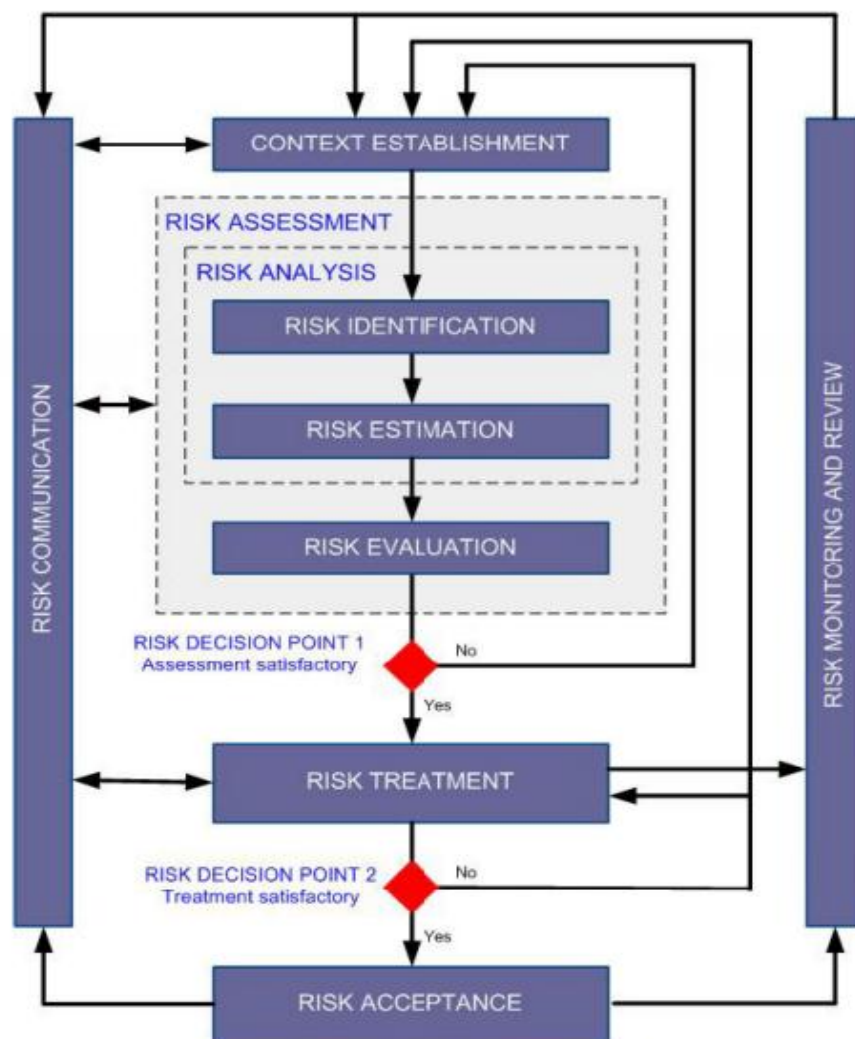


Figure 2. Information security risk management process [41]

2.2.2.2 OCTAVE Method

OCTAVE started as a team of risk evaluation experts that performs Information Risk Evaluation for organizations. As a result of experiences gathered over the years, the team developed a framework called OCTAVE. This framework was first published in June 1999. This refined framework was specifically developed for large organizations and a new method targeting smaller organizations was later developed [25].

The OCTAVE information security risk management framework describes 6 steps in managing security risks. The steps are - Identify risk, Analyze risk, Plan, Implement, Monitor and Control.



Figure 3. OCTAVE Information Risk Management Framework [25]

Identify risk: this phase involves profiling of risks and gathering of information relating to each component that makes up the risks. Assets are classified according to their values to the organization. Critical assets are identified and security requirement outlined for each critical asset identified. Also organizational information that are related to the risk profiles are captured and recorded. Such organizational information usually includes current security, policies, practices, and procedures.

Analyze: the analysis phase is divided into two; the first step is evaluate the risks while the second step is to prioritize the risks. The value of these risks is determined by measuring the impact and probability of identified risk components. Prioritization of risk is achieved by deciding which of the risks must be addressed and mitigated. The priorities are determined based on organizational goals and objectives as it relates with the risk identified.

Plan: the planning phase involves mapping out strategies and plans for combating the identified risk. At this phase, risk protection strategies and risk mitigation plans are developed. The action plan for implementing these strategies is mapped out. The action plan covers budget, schedule, success criteria, monitoring measures, personnel assigned for plans implementation.

Implementation: this phase involves assigning specific activities in the action plan to individual staff members.

Monitor: at this phase, activities in the action plan are monitored in respect to goals and deadlines assigned for achieving objectives.

Control: at the concluding phase, the key results from the monitoring process such as progress reports and risk indicators are analyzed. Decisions regarding identification of new risks are made based on result of the analysis and the entire process starts all over again.

In this master thesis, our areas of concentration are on identification of risks, analysis of risks and security requirement for managing and mitigating risks. The ISSRM Domain provides a method to achieve this goal. The ISSRM Domain model is closely related to the first and second phase of the OCTAVE framework and is described below.

2.2.2.3 Information System Security Risk Management Domain Model

The ISSRM provides a method for analyzing, evaluating and quantifying information security risks. ISSRM Domain Model is a conceptual model in the form of UML class diagram providing reference for the assessment of security-oriented models [24]. The framework is broken down into 3 concepts; Assets related concepts, risk related concepts and risk-treatment related concepts.

Table 2. ISSRM Domain Model Concepts [24]

Type	Concept	Name
Asset-related concepts	(1)	Asset
	(2)	Business asset
	(3)	IS asset
	(4)	Security criterion
Risk-related concepts	(5)	Risk
	(6)	Event
	(7)	Impact
	(8)	Threat
	(9)	Vulnerability
	(10)	Threat agent
	(11)	Attack method
Risk treatment-related concepts	(12)	Risk treatment
	(13)	Security requirement
	(14)	Control

Assets related concepts

Assets are grouped into business assets and information system assets. Security criteria for each business asset are defined. Security criteria are properties of a business asset characterizing its security needs and they are - availability, integrity and confidentiality.

Risk Related Concepts

Risks and all risk components are defined under this concept. The components are summarized as follows -

Impact: possible negative consequence of risk to an organization.

Vulnerability: attribute of an IS asset that constitutes security weakness.

Threat agent: an agent with a possibility of causing harm in the system.

Threat: a possible attack executed by an agent which may cause harm to assets.

Event: resulted by combining threats with one or more vulnerabilities.

Attack method: means by which a threat agent executed the attack.

Risk Treatment related concepts

A risk treatment concept explains the decision on how risk is treated in order to satisfy security needs. The treatment of a potential risk can be achieved by the following avoiding risk, transferring risk, reducing risk, and retaining risk.

Security requirement: defines a condition that must be satisfied before the security criteria are achieved.

Control: they are processes, policies, procedures mapped out to improve security as specified by security requirement.

A Universal Modeling Language (UML) class diagram of ISSRM domain model describes relationship between the concepts described above. It shows how various risk components are systematically linked to each other.

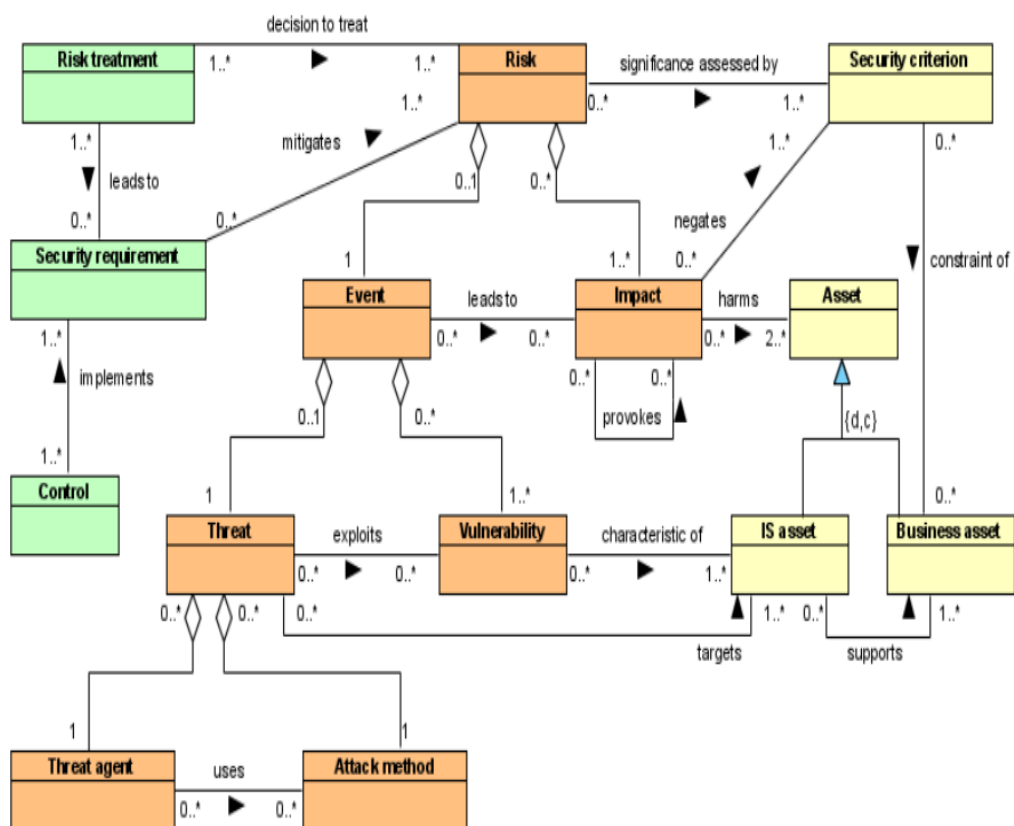


Figure 4. ISSRM Domain Model [29]

The ISSRM Domain model on its own does not provide a method for estimating risks. However, the ISSRM Domain model can be combined with Goal Question Metric (GQM) to provide a mathematically reliable way for measuring and quantifying the value of risk components.

2.2.2.4 Goal Question Metric Framework

The GQM method developed by V. Basili and D. Weis provides means of measurement in a top-down approach and the focus is based on goals and models [26]. The method can be described in three levels:

Conceptual level (Goal): this is represented by an object in form of a product, process or a resource.

Operational level (Question): question used to describe a specific goal.

Quantitative level (Metric): data providing answers to the goal questions in a quantitative and measurable way.

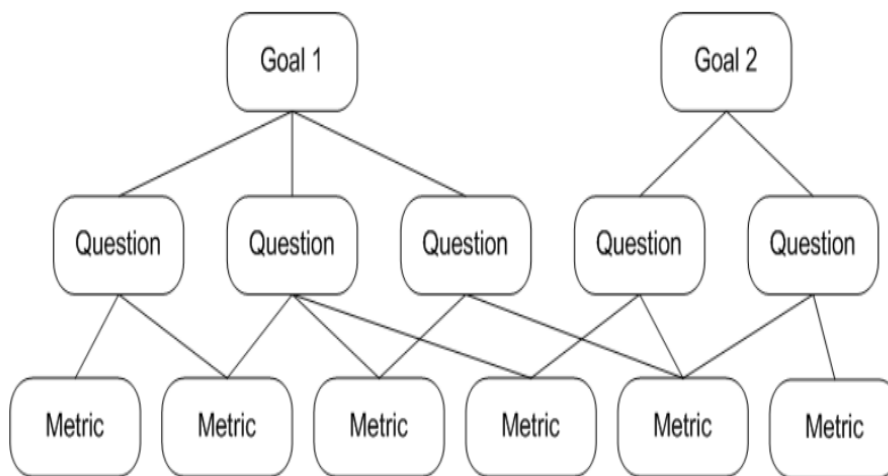


Figure 5. Example of GQM Model [26]

The GQM when applied in relation to the ISSRM Domain Model, two possible Goals can be generated [24]

- Maximization of risk reduction
- Minimization of risk treatment cost

For maximizing risk reduction goal, questions derived and metrics for measurement is shown in the figure below:

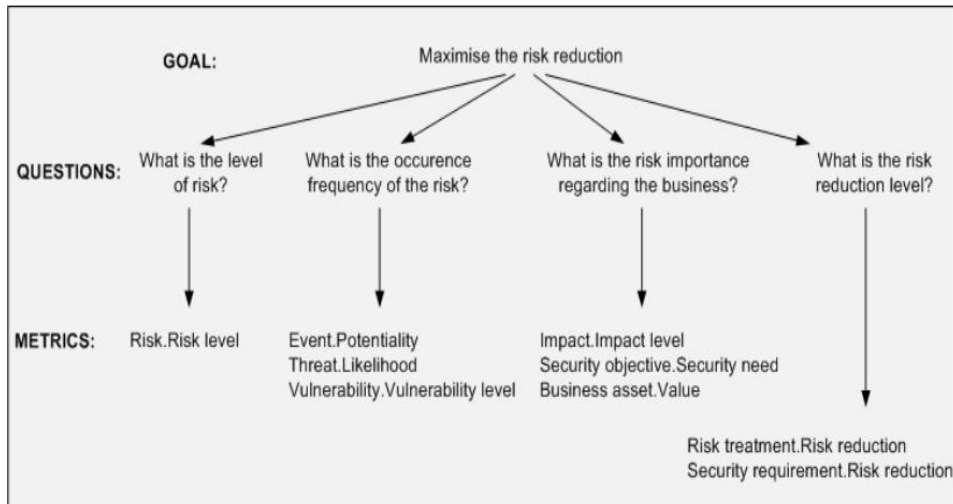


Figure 6. GQM risk reduction maximizing goal [24]

In minimizing risk treatment cost, the question generated can be asked as thus: What is the risk treatment cost?

The metrics list out cost related to risk treatment such as security requirement cost and control cost.



Figure 7. GQM Risk Treatment minimizing goal [24]

3 Identification of Assets in Enterprise Collaboration

In order to analyse security threats in enterprise collaborations, the first step is to identify assets involved in this collaboration. In this chapter, our goal to analyse and identify assets involved in collaboration between airline and service providers.

This is in line with the general goal of this thesis that is how to analyse digital security threats in enterprise collaboration. This chapter is solely dedicated to finding answers to research question number one:

RQ1: How to identify relevant assets in enterprise collaborations that need to be secured?

The main research goal of this chapter is broken down into two what questions:

RQ1.1: What IT Systems are involved in these collaborations?

RQ1.2: What information is exchanged between collaborating systems?

The first sub question RQ1.1 is answered in section 3.1 that discusses Airline day of Operation (DOO). The area of concentration on this thesis is on turnaround workflow of airline DOO. Therefore specific questions regarding IT systems involved in the collaboration is identified in section 3.1.3 which discusses the airline turnaround workflow.

The second research question is answered in section 3.2. The airline turnaround workflow and the processes that make up the airline turnaround are described in detail. Business assets which contain information that are exchanged between the airline and service providers are identified and analyzed. The analyses are based on identifying the value and the data that are contained in these assets.

3.1 Airline Day of Operation

The airline day of operation shows routine tasks and workflows before takeoff and after takeoff flights. Because of scope of this work and area covered in [21], the following processes are considered flight preparation, turnaround and takeoff.

3.1.1 Flight Preparation

This phase involves gathering and compiling of flight plans for all proposed flight. The flight plan is a document that describes a proposed aircraft flight.

3.1.2 Takeoff

The takeoff activities are the last set of pre-flight activities to be carried out before the actual takeoff of flight. The activities include reviewing of flight plans, load balancing and calculation of additional fuel required. This phase ends with the approval of flight plan and requesting of takeoff clearance from the Air Traffic Control (ATC).

3.1.3 Turnaround

This phase of operations generally involves the following set of activities - ground operations, passenger management and gate agent activities. The ground operations encompass all activities that take place before the passengers start boarding the aircraft. Cargo and luggage offload, aircraft cleaning, restocking of aircraft, refueling and loading of cargo and luggage.

Passenger management comprises of passenger check and luggage check-in activities. The Gate agent monitors the ground operations activities and passenger management activities.

Out of all the airline day of operation workflows described, the turnaround phase provides more opportunities for collaborations between the airline and service providers. This is because the activities involved in this phase are resource intensive and are not part of the core competence of the airlines.

The diagram in figure 7 shows information systems that support collaboration activities in the turnaround workflow as follows –

Passenger management: this is an IS asset because it contains activities, participants, business entities, roles and rules in passenger management pool of the turnaround workflow.

Ground operations: it is made up of activities, business entities etc. in the ground operations pool of turnaround workflow.

Messaging system: the messaging system is made up of rules, protocols, networks that determine how digital information is transmitted between airline and service providers. The Domain Name Servers (DNS) and Simple Mail Transfer Protocol (SMTP) are

examples of networks and protocols that play a role delivery of messages from sender to receiver.

Passenger check-in process: this IS asset contains rules, procedures etc. on how passengers are checked-in to board the flight.

Luggage check-in process: this IS asset contains rules, procedures etc. on how luggage are checked-in to the aircraft.

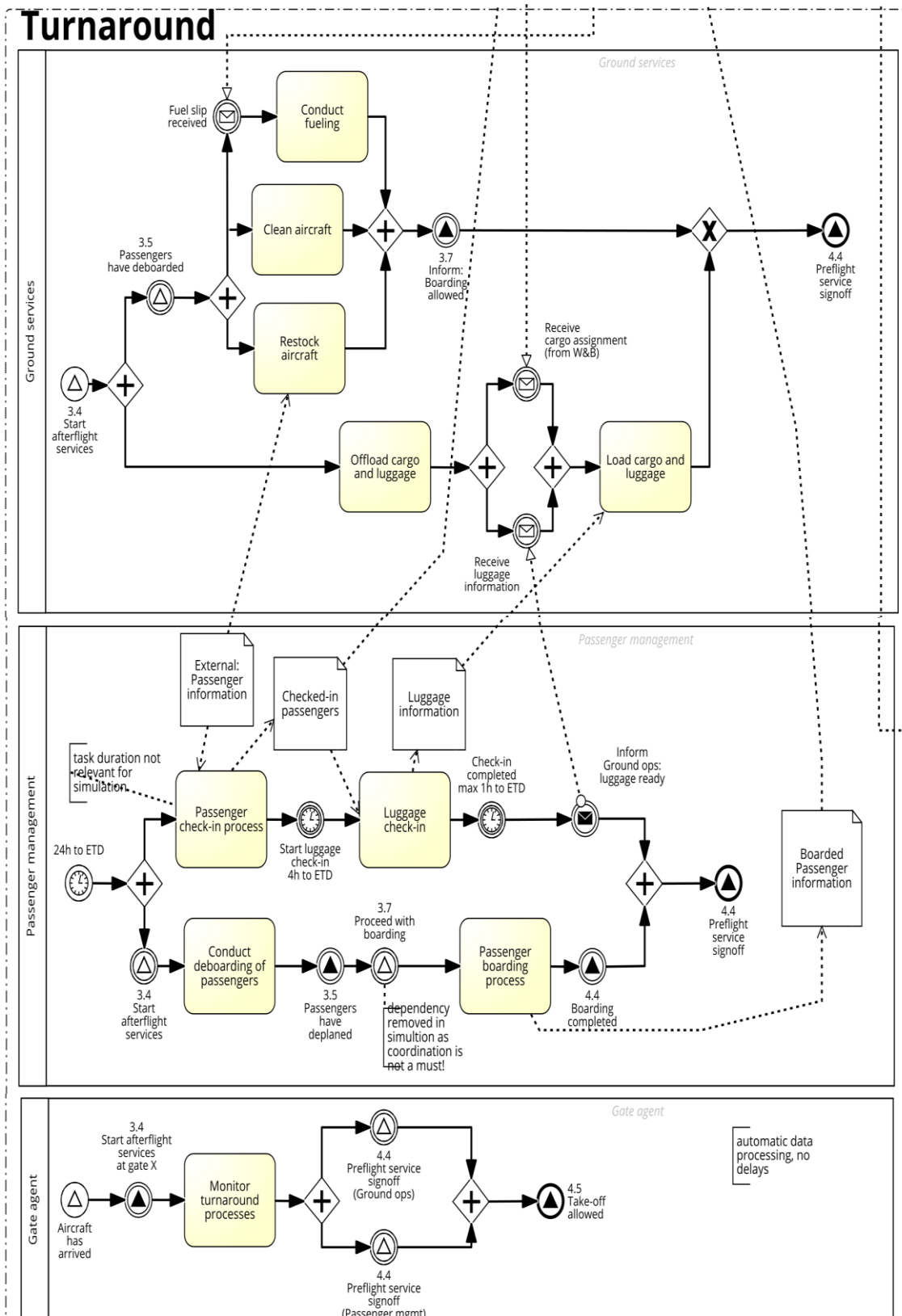


Figure 8. Airline turnaround phase of day of operation [43]

3.2 Assets in Airline Turnaround workflow

Figure 8 describes a knowledge model for airline turnaround. It comprises of the following roles - passenger management and ground operations. Each set of activity generates a specific data objects and can also trigger other set of activities.

3.2.1 Passenger Management Process

Different forms of passenger data are generated throughout the passenger management process. Such data may include names, addresses, phone numbers etc. Other data contained may include frequency of travel, destination and hotel reservations of travellers. The value of these information are significant to the airlines because these data contains details that completely describe the customers of the airline. Customers (information) are intangible business assets which must be valued and properly managed [34], and therefore there is need to secure customer's personal information as a business asset.

The asset identification starts by identifying information systems assets that support business assets in the passenger management process in airline turnaround workflow. A process description outlining possible activities involving the business asset is shown in the asset identification tables. The security criteria for each of the business asset identified in the passenger management process are also stated in asset identification tables. Passengers information are contained in the following data objects – checked-in passenger information and luggage information.

3.2.1.1 Checked-in passenger information: This data object is generated during the check-in activity and contains data about passengers that checked-in for a flight. The data may include time of check-in, seat reservations, and other special requests by passengers. The passenger information also contains personal details such as name, passport number, address, contact, next of kin etc. An attacker with access to these information can successfully conduct social engineering or phishing attacks on airline passengers.

The *check-in* activity represents the IS asset which supports the business asset *Checked-in passenger information*. An attacker can manipulate the passenger check-in process and this may cause blacklisted individuals to be able to board the aircraft.

Table 3. Checked-in passenger information asset Identification

Assets	Business assets IS assets	Checked-in passenger information Passenger check-in process Passenger management Passenger Check-in Personnel	
Process description	IS assets	Passenger physical check-in process: <ul style="list-style-type: none"> • Passenger goes to the check-in personnel • Passenger provides Identification document • Personnel verifies Identity document • Personnel prints out boarding-pass • Passenger collects boarding-pass 	Passenger online check-in process: <ul style="list-style-type: none"> • passenger visits the online check-in portal • enters booking number and confirms check-in • passenger prints boarding-pass
Security Criteria		Confidentiality of checked-in passenger information.	

The table above shows details about information system asset that supports the business asset - checked-in passenger information. The table also descriptions of procoesses involving the business asset which are physical check-in process and online passenger check-in process. The security criterion for the business asset is also identified as

confidentiality of checked-in passenger information. Confidentiality of information is necessary because it is important that data contained in checked-in passenger information are only available people who should have access to it.

3.2.1.2 Luggage information: The data object is created in the luggage check-in activity, which starts at the end of passenger check-in activity. The luggage information is transmitted via messaging system to the ground services to generate cargo assignment information. The data object contains details about baggage carried by different passengers. These may include size, weight and content of passenger baggage. The *check-in* activity and the *messaging system* represent the IS asset tasks that supports the business asset *Luggage information*. An attacker can manipulate the luggage check-in process which may cause luggage with dangerous substances to be loaded to the aircraft.

Table 4: Luggage information asset identification table

Assets	Business assets IS assets	Luggage information Luggage check-in process Messaging system Passenger management
Process description	IS assets	Luggage check-in process description <ul style="list-style-type: none"> • passenger drops the luggage after passenger check-in process • personnel measures luggage to confirm if it meets requirement • personnel records the weight and size • personnel drops the luggage for loading into aircraft
Security Criteria		Confidentiality of luggage information

	Integrity of luggage information
--	----------------------------------

The table above shows details about luggage information business asset. It starts by identifying the IS assets that support the luggage information which are luggage check-in process, the passenger management pool, and the messaging system. The security criteria for the asset are identified as confidentiality of data and integrity of data. This is important because it is necessary that the data contained in luggage information are only available to the right persons and also remain unchanged.

3.2.2 Ground Operations

The following assets are involved in ground operations.

3.2.2.1 Fuel-Slip: After passengers have completely de-boarded the aircraft, a fuelslip is sent via messaging system to an external provider to start the refueling activity. The fuelslip contains details about quantity and quality of fuel to be loaded in various fuel tankers of the aircraft. The *messaging system* represents the IS asset that supports the *fuelslip* business asset.

The quantity of fuel and distribution in the aircraft is very crucial in even spreading of weight across the aircraft and maintaining proper load balancing in the aircraft. Load balance control refers to the location of the Centre of Gravity of an aircraft and this is of primary importance to aircraft stability, which determines safety in flight [35].

The data contained in the fuel receipt can be maliciously changed by an attacker. The quantity of fuel on the fuel receipt can be change and may result to insufficient fuel to be loaded on the aircraft. It is also possible that an attacker changes the type and quality of fuel on the fuel receipt and this can cause the aircraft to be loaded with the wrong fuel. However, if wrong quantities of fuel are loaded on different fuel tankers of the aircraft, it can cause the centre of gravity of the aircraft to shift beyond allowable limit. This can cause the aircraft to lose stability and spin in midair [35]. Loading an aircraft with the wrong type of fuel results in failure of the engines of the aircraft and can result in air crash [36].

Table 5: Fuelslip asset Identification table

Assets	Business assets IS assets	Fuelslip Messaging system, Ground operations
Process description	IS assets	Description of the process of sending fuelslip to service provider: <ul style="list-style-type: none"> • Service provider receives fuelslip. • Conducts refueling based on data contained in fuelslip.
Security Criteria		Integrity of fuelslip

The fuelslip asset identification table shows details of IS assets that support the fuelslip, process description that involves the fuelslip and security criterion for the fuelslip. Two IS assets supporting the fuelslip business asset are messaging system and ground operations pool. The security criterion is identified as integrity of data. It is necessary that data contained in the fuelslip document remains unchanged in the course of airline turnaround.

3.2.2.2 Cargo assignment: On the completion of offload of cargo and luggage, cargo assignment information is sent via messaging system to the external provider to commence loading of new cargo and luggage to the aircraft. The cargo assignment holds data about weight of baggage, luggage and other checked-in cargos. The cargo weights as well as passengers and fuel weights are necessary in maintaining centre of gravity and stability of the aircraft. The messaging system represents the IS asset that supports the business asset *cargo assignment*.

An attacker can change the values of data contained in the cargo assignment and can cause the aircraft can be overloaded beyond acceptable weight level. This can reduce

the efficiency of the aircraft and also reduce the safety margin available if an emergency condition should arise [35]. The reduction in efficiency of the aircraft can result to the following - higher takeoff speed, longer takeoff run, reduced rate and angle of climb, lower maximum altitude, shorter range, reduced cruising speed, reduced maneuverability, higher stalling speed, higher landing speed, longer landing roll¹.

Table 6: Cargo assignment asset identification

Assets	Business assets IS assets	Cargo assignment Messaging system Ground operations
Process description	IS assets	Description of the process of sending cargo assignment to service providers: <ul style="list-style-type: none"> • Service provider receives cargo assignment document. • Aircraft is loaded with cargoes and luggage based on data contained on cargo assignment document.
Security Criteria		Integrity of cargo assignment

The cargo assignment asset identification table above shows the IS assets that supports business assets, process description involving the business asset and security criterion for the business asset. The IS assets are messaging system and ground operation pool while the security criterion is integrity of cargo assignment.

¹ Annex of Weighing-systems.com, describing deficiencies of aircrafts as a result of too much weight <http://www.weighing-systems.com/TechnologyCentre/aircraftweighing.html>

3.3 Conclusion

This chapter is focused on identifying assets involved in enterprise collaboration in the aviation industry. Since the turnaround workflow presents more opportunities for collaboration because of the resource intensiveness of the processes in the workflow, therefore airline turnaround workflow is chosen as a case study.

The processes which involve collaboration with service providers in airline turnaround are ground operations and passenger management process. The business assets in these two processes were identified and IS assets that support these assets were also identified. A process description involving the identified assets and security criteria for the assets were also outlined in the tables in this chapter.

The analyses performed in this chapter are based on processes identified in the airline turnaround workflow. This is because the turnaround operations are resource intensive and presents more opportunity for collaboration between airlines and service providers in airlines day of operations. The processes identified for analysis are Passenger management and Ground operations of the turnaround workflow. Assets involved in these processes are identified and grouped into business assets and information systems assets.

4 Risk analysis of assets in turnaround workflow

The goal of this chapter is to apply ISSRM Domain Model in analyzing security risks identified in passenger management process and ground operation process in airline turnaround workflow. This is relevant to the main objective of this thesis which is to analyze digital security threats in enterprise collaborations.

The analyses performed in this chapter provide answers to the research question which is stated as follow –

RQ2: How do security risks threaten collaboration systems?

The research question RQ2 is further broken down into the following sub-questions

RQ2.1: What are the threat agents?

RQ2.2: What are vulnerabilities?

RQ2.3: What are attack methods?

RQ2.4: What are the risk impacts?

Answers to the research questions RQ2.1, RQ2.2, RQ2.3 and RQ2.4 are provided in passenger management risk analysis in section 4.1 and ground operations risk analysis in section 4.2

The ISSRM domain model is an information risk management framework for the assessment of security-oriented modeling languages [24]. The analyses are performed based on the 3 concepts that ISSRM Domain model is built up on: assets related concepts, risk related concepts and risk-treatment related concepts.

For each of the asset identified in the passenger turnaround process, two possible risk scenarios are evaluated. The risk components - threat agent, attack method, threat, vulnerability, event, and impact are systematically derived from the process description of the identified assets.

4.1 Passenger Management Risk Analysis

The assets identified in passenger management process of airline turnaround workflow are analyzed in the tables below. The assets identified are as follows -

- Checked in passenger information
- Luggage information

The risk analysis of assets in passenger management starts by identifying potential attackers of the passenger management system, their motivation and the resources which they possess. With this information in place, then an analyst can easily describe a process of how a potential attacker can carry out an attack on the passenger management part of airline turnaround workflow.

The risk analysis tables identify the risk components of assets in passenger management process. The risk components which are threat agent, attack method, threat, vulnerability, event, and impact are outlined in each of scenario described in the asset identification table of passenger management.

4.1.1 Checked-in passenger risk analysis – two possible attack methods are described for the checked-in passenger information business asset. Each of the attack method has its own threat agent. The table 7 describes each of the threat agent, the attack method and risk components of the check-in passenger information.

Table 7: Checked-in passenger information risk and threat analysis

	A	B
Threat Agent	<p>Blacklisted passenger</p> <p>Motivation: need to board the flight.</p> <p>Resources: fake ID, money to bribe the check-in personnel.</p>	<p>An attacker</p> <p>Motivations: need to board the flight, sabotage the reputation of the airline and cause airline passengers to miss their flights.</p> <p>Resources: fake check-in website,</p>

	Expertise: knowledge of the check-in process	passengers data. Expertise: knowledge of check-in process, knowledge email phishing attacks.
Attack Method	<ul style="list-style-type: none"> • Bribes personnel to steal checked-in passenger information. • Presents fake ID at the check-in desk • Gets checked in with fake ID and checked-in passenger information 	<ul style="list-style-type: none"> • Attacker sends phishing email to passengers that booked a flight. • Passenger enters booking number to the fake check-in website and checks in. • Passenger prints a fake boarding-pass with flight time changed to few hours ahead of the actual flight time • Attacker uses passenger booking number to check-in to the original site and prints boarding-pass • Attacker boards the flight with the original boarding pass • Passenger misses flight
Threat	Blacklisted passenger bribes the personnel, presents fake ID, and gets checked-in.	Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight.
Vulnerability	Check-in personnel could be bribed.	Passenger cant differentiate between original and fake check-in website
Event	Blacklisted passenger presents	Attacker uses phishing email to

	fake document, bribes personnel and gets checked-in because check-in personnel could be bribed.	extract passenger booking number and uses it to check-in to the flight because passenger can't differentiate between original and fake check-in website.
Impact	<ul style="list-style-type: none"> • Loss of confidentiality of checked-in passenger information. • Passenger check-in process can no longer be trusted. • Checked-in passenger information is stolen. 	<ul style="list-style-type: none"> • loss of trust in online check-in process • passenger information is stolen • passenger misses flight
Risk	Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed which results to loss of confidentiality of checked-in passenger, loss of trust in check-in process and stolen checked-in passenger information.	Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight because passenger cant differentiate between original and fake check-in website which causes the passengers to miss their flight, their information stolen, resulting to loss of trust in the airline and its online check-in process.

The analysis in the table above starts by identifying two potential threat agents as – blacklisted passenger and an attacker. For the blacklisted passenger, his motivation to carry out an attack on check-in passenger information could be the need to board the flight which he is already blacklisted. For a random attacker, his motivation could be to sabotage the reputation of the airline by causing the passengers to miss their flights. The two possible attackers have knowledge of how the airline check-in process works. The attacker that wants to harm the reputation of the airline will also need a fake website site to carry out a phishing attack on the passengers of the airline.

The table also outlines step-by-step details on how these two attacks can be carried out on the checked-in passenger information. The first attack method describes a physical passenger check-in process while the second attack description shows attack on online check-in. The vulnerability in the online check-in process is the passenger ignorance of the genuine check-in website. For the physical check-in process, the check-in personnel could be bribed. By successfully taking advantage of these weaknesses, an attacker can board a flight with passenger’s information or even cause the passenger to miss the flight.

These two attacks negatively affect the airline check-in process. The attacks can cause the passengers to lose trust in the passenger check-in process and also passengers’ data are stolen in the course of the attack. Specifically for the second attack, the passenger can miss their flight as a result of the attack.

4.1.2 Luggage information risk analysis – two possible attack methods are described for the luggage information business asset. The same possible threat agent – luggage check-in personnel is identified for these two attacks. The table 8 describes each of the threat agent, the attack method and risk components of the luggage information asset.

Table 8. Luggage information risk analysis table

	A	B
Threat Agent	<p>Luggage check-in personnel</p> <p>Motivation: Sabotage the safety of the flight.</p> <p>Resources: weighing machine, luggage information document.</p> <p>Expertise: Knowledge about luggage check-in process.</p>	<p>Luggage check-in personnel</p> <p>Motivation: hide contraband item on passenger luggage.</p> <p>Resources: has physical access to the luggage.</p> <p>Expertise: knowledge of the check-in process and messaging system.</p>
Attack	<ul style="list-style-type: none"> Personnel accept luggage and 	<ul style="list-style-type: none"> Personnel accept and weigh

Method	<p>measure luggage.</p> <ul style="list-style-type: none"> Records values lower than actual weight of luggage. Sends luggage information to ground services for onward loading of the aircraft. 	<p>luggage.</p> <ul style="list-style-type: none"> Adds contraband item to passenger luggage and record the weight of luggage Sends luggage information to ground services for onward loading of the aircraft.
Threat	Personnel measures and records values lower than actual weight of luggage, sends luggage and luggage information to ground operations for onward loading of the aircraft	personnel accepts luggage and adds contraband item to passengers luggage, sends luggage and luggage information to ground operations to load the aircraft
Vulnerability	Luggage information generated by the check-in personnel is not verified	personnel activity is not monitored
Event	Personnel records values lower than actual weight of luggage, and ground operations uses the information in the loading of the aircraft because luggage information generated by personnel is not verified	personnel accepts luggage and adds contraband item to passengers luggage, sends luggage and luggage information to ground operations to load the aircraft because personnel activity is not monitored
Impact	<ul style="list-style-type: none"> Loss of integrity of luggage information. Incorrect calculation of centre of gravity (cg) of aircraft. 	<ul style="list-style-type: none"> Loss of integrity of contents of passenger luggage. Loss of trust in luggage check-in process.
Risk	Personnel records values lower than actual weight of luggage, and ground operations uses the	Personnel accepts luggage and adds contraband item to passengers luggage, sends

	<p>information in the loading of the aircraft because luggage information which results to loss of integrity of luggage information and incorrect calculation of cg of which might cause aircraft to be unstable .</p>	<p>luggage and luggage information to ground operations to load the aircraft because personnel activity is not monitored which results to loss of integrity of contents of passenger luggage and loss of trust in luggage check-in process.</p>
--	--	---

The motivation of the luggage check-in personnel to carry out the first attack is to sabotage the safety of the flight. The attacker has knowledge of how the luggage check-in process works, and also has access to the documents for recording details about the luggage. To carry out the attack, the personnel have to manipulate the records in the luggage document so that the aircraft will be overloaded.

The motivation of the personnel to carry out the second attack on the airline is to hide contraband item in the passenger luggage. This he can achieve because he has physical access to the passenger luggage and also knows how the luggage check-in process works.

The vulnerabilities present in the luggage check-in process for these two attacks to be possible is as follows - data generated by the check-in personnel is not verified and activities of the check-in personnel are not properly monitored.

The impact of these two attacks are as follows – for the first attack, its leads to loss of integrity in data contained in luggage information and also leads to overloading the aircraft. For the second attack, the impact is that passengers loose trust in the luggage check-in process and loss of integrity of the contents of passengers’ luggage.

4.2 Ground operations risk analysis

The assets identified in ground operation process of airline turnaround workflow are analyzed in the tables below. The assets identified are as follows – fuelslip and Cargo assignment

Risk components in assets in ground operations are shown in the risk analyses tables. The risk components are outlined in each of scenario described in the asset identification table of ground operation process of the airline turnaround workflow.

The risk treatment tables show the security requirements and controls that must be applied in order to reduce the risks or totally avoid the risks identified in the risk analysis tables of ground operation process.

4.2.1 Fuel-slip risk analysis – for the fuel-slip risk analysis, two possible attack methods are described for this business asset. For each of these attacks, two possible threat agents are identified - a malicious insider and an arbitrary attacker. The table 9 below describes the threat agents, the attack methods and risk components of the fuelslip asset.

Table 9: Fuelslip risk and threat analysis

	A	B
Threat Agent	<p>Malicious insider</p> <p>Motivation: sabotage the safety of the flight</p> <p>resources: access to fuelslip document</p> <p>expertise: knowledge of refueling process</p>	<p>An attacker</p> <p>Motivation: sabotage the safety of the flight</p> <p>resources: access to airlines messaging system and mailing list</p> <p>expertise: knowledge of refueling process</p>
Attack Method	<ul style="list-style-type: none"> • Malicious insider accesses computer storing fuelslip documents. • Makes changes to the content of fuelslip. • Fuelslip is sent to the service provider. 	<ul style="list-style-type: none"> • Attacker intercepts fuelslip. • Airline sends fuelslip to attacker. • Attacker changes data contained in fuelslip • Attacker sends edited fuelslip to supplier. • Supplier conducts refueling based on

		information in fuelslip received.
Threat	Malicious insider access the fuelslip document and changes the data contained in the document.	Attacker intercepts fuelslip, receives fuelslip, changes data contained, sends to supplier, refueling is conducted based on information on fuelslip.
Vulnerability	fuelslip document is not encrypted	Email message can be intercepted.
Event	Malicious insider with access to computer that stores fuelslip make changes to the data contained in fuelslip before it is sent to service provider because the document is not encrypted.	Attacker intercepts fuelslip, receives fuelslip, changes data contained, sends to supplier, refueling is conducted based on information on fuelslip because email message can be intercepted.
Impact	<ul style="list-style-type: none"> • Loss of integrity of fuelslip • Lower quantity or different type of fuel can be loaded to the aircraft. 	<ul style="list-style-type: none"> • Loss of integrity of fuelslip. • Data contained in fuelslip can be changed.
Risk	Malicious insider with access to computer that stores fuelslip make changes to the data contained in fuelslip before it is sent to service provider because the document is not encrypted which results to loss of integrity of fuelslip and can cause the aircraft to be loaded with wrong	Attacker intercepts fuelslip, changes data contained, sends to supplier, refueling is conducted based on information on fuelslip because messaging system can spoofed, which causes loss of integrity of fuelslip

	quantity and type of fuel.	and can result in loading the aircraft with wrong quantity and type of fuel.
--	----------------------------	--

From the table above, the goal of the malicious insider to carry out the first attack is to sabotage the safety of the flight. The Malicious insider has access to fuelslip document and has expert knowledge of the airline refuelling process. The malicious insider can make changes to the fuelslip document, and when the service provider loads the refuels the aircraft with the service requirement in the fuel, the aircraft will be loaded with the wrong fuel.

For the second attack, a random attacker with a help of an insider can manipulate the messaging system and intercept fuelslip document. The motivation is the same and that is to sabotage the safety of the aircraft. The fuelslip is transmitted via the messaging system to the service provider. An attacker (with the help of an insider), can intercept the fuelslip and modify data contained in it. In the event of successful exploitation of this weakness, the effect is that the aircraft is loaded with the wrong type or quantity of fuel.

The weakness in the system for these attacks to be possible is because the fuelslip document is not encrypted and the email messages between airline and service providers can be intercepted. These two attacks negatively affect the airline by causing loss of integrity of fuelslip document and also possibly resulting in the aircraft to be loaded with the wrong fuel.

4.2.2 Cargo assignment risk analysis – There are two possible attacks that are described for cargo assignment business asset. The threat agents for each of these attacks are malicious insider and a random attacker. The table 10 below describes each of the threat agent, the attack method and risk components of the fuelslip asset.

Table 10. Cargo assignment risk analysis

	A	B
Threat Agent	<p>Malicious insider</p> <p>Motivation: sabotage the safety of the aircraft.</p> <p>Resources: access to cargo assignment document.</p> <p>Expertise: knowledge of luggage and cargo loading process</p>	<p>An attacker</p> <p>Motivation: sabotage the safety of the flight.</p> <p>Resources: access to airlines messaging system and mailing list.</p> <p>Expertise: knowledge of cargo loading system</p>
Attack Method	<ul style="list-style-type: none"> • Access the cargo assignment document. • Make changes to the cargo assignment document. • Changed cargo assignment is sent to service provider 	<ul style="list-style-type: none"> • Attacker hacks airlines mailing list. • Attacker replaces service provider email with his email. • Airline sends cargo assignment to attacker. • Attacker changes data contained in cargo assignment. • Attacker sends edited assignment to service provider. • Service provider conducts cargo and luggage loading based on information in cargo assignment document received.

Threat	Malicious insider with access to cargo assignment document make changes to cargo assignment document before it is sent to service provider.	Attacker hacks airline mailing list, receives cargo assignment, changes data contained, sends to service provider, loading is conducted based on information on cargo assignment.
Vulnerability	Cargo assignment document is not encrypted.	Mailing list is not fully secured.
Event	malicious insider with access to cargo assignment document make changes to cargo assignment document before it is sent to service provider because cargo assignment document is not encrypted	Attacker hacks airline mailing list, receives cargo assignment, changes data contained, sends to service provider, loading is conducted based on information on cargo assignment because mailing list is not fully secured
Impact	<ul style="list-style-type: none"> • Loss of integrity of cargo assignment document. • Aircraft is not properly loaded. 	<ul style="list-style-type: none"> • Loss of cargo assignment slip • Data contained in cargo assignment can be changed
Risk	Malicious insider with access to cargo assignment document make changes to cargo assignment document before it is sent to service provider because cargo assignment document is not encrypted which causes loss of integrity of cargo assignment and improper loading of the aircraft and can result to instability of the aircraft in the air.	Attacker hacks airline mailing list, receives cargo assignment, changes data contained, sends to service provider, loading is conducted based on information in cargo assignment, because mailing list is not fully secured which causes loss of integrity of cargo assignment and can

		result to overloading the aircraft.
--	--	-------------------------------------

The goals of the attacks in the table above are the same – to sabotage the safety of the aircraft. For the first attack, the malicious insider has access to the cargo assignment document and also has the knowledge of aircraft loading process. To carry out the attack, the malicious insider changes data contained in fuelslip before it is sent to the service provider to reload the aircraft. The service provider loads the aircraft with the information in the cargo assignment.

The second attack involves intercepting of the cargo assignment document as it sent from airline to the service provider. This the attacker can achieve by hacking the airline mailing list so that he can receive email sent to the service providers. By intercepting and changing data contained in cargo assignment before it gets to the service provider, the aircraft will be reloaded improperly.

The vulnerabilities that results in these attacks are as follows – the cargo assignment document is not encrypted and the mailing list is not properly secured.

These attacks will affect the airline negatively because of the loss of integrity of fuelslip document resulting from the attack. Also, the attack can cause the aircraft to be improperly loaded.

4.3 Conclusion

In this chapter, assets identified in chapter 3.0 were analysed to determine security risks on each of them. To determine the risks on these assets, the risk components of the assets were identified. The risk components are – threat agent, attack method, threat, vulnerability, risk event and impact. The risks were derived by systematically combining the risk components of the each asset.

In the tables of this chapter, two possible scenario labelled column A and B were outlined respectively. As a result, two possible risks were derived for each of the identified assets.

The risk analyses are performed based on the risk components which are – threat, threat agent, vulnerability, attack method, event and impact. The risk is derived by

systematically identifying all risk components from the process described section 3.2 and summing the risk components.

5 Treatment and Evaluation of Risk

The goal of this chapter is to apply security controls to manage the security risks identified in chapter four. Evaluation is also performed to estimate how the risks were reduced as a result of application of security controls. The evaluation is performed in two steps – evaluating risk components before introducing security components and evaluating risk components after introducing security controls.

The security controls and risk evaluations provide answer to the research question – RQ3: How to mitigate security risks in enterprise collaborations?

The research question RQ3 is further broken down into the following sub-questions -

RQ3.1: What are the security requirements?

RQ3.2: What are the security controls that implement the security requirements?

RQ3.3 What degree of security is achieved with implementing the security controls?

The answers to the research questions RQ3.1 and RQ3.2 are provided in risk treatment in section 5.1 and the research question RQ3.3 is answered in section 5.2

5.1 Risk treatment

The risks identified in chapter four are managed by applying security requirement and controls. The security requirement and controls mitigate the risks either by eliminating them completely or by reducing the effects on the asset. However, for the purpose of this work, our emphasis is on security requirement and controls that reduces the risk to an acceptable level. An estimated cost of countermeasures is provided for each of the security control applied on the risk. The cost of risk treatment is estimated from 1 to 5.

In this section, the risk treatment for airline turnaround workflow is divided into four stages. The four stages are based on assets identified in ground operations and passenger management process of turnaround workflow and they are – the passenger information risk treatment shown in section 5.1.1, the luggage information risk treatment in section 5.1.2, the fuel-slip risk treatment in section 5.1.3 and cargo assignment risk treatment in section 5.1.4

5.1.1 Passenger Information Risk Treatment

From the risk analysis performed in chapter four, the following risks are identified in the passenger information asset -

Risk 1: *Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed which results to loss of confidentiality of checked-in passenger, loss of trust in check-in process and stolen checked-in passenger information document is not encrypted which causes loss of integrity of cargo assignment and improper loading of the aircraft and can result to instability of the aircraft in the air.*

Risk 2 : *Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight because passenger cant differentiate between original and fake check-in website which causes the passengers to miss their flight, their information stolen, resulting to loss of trust in the airline and its online check-in process.*

Table 11: Checked-in passenger information risk treatment table

	Risk 1		Risk 2	
Risk treatment	Treatment cost	Risk reduction	Treatment cost	Risk reduction
Security requirement		Monitor the activity of check-in personnel		Educate the airline passengers on phishing attacks.
Controls	4	Officer verifying the actions of check-in personnel	2	Using secured https websites for booking and check-in activity.

In the table above, the security requirement needed to reduce Risk1 is accomplished by monitoring the activities of check-in personnel. In order to achieve this security requirement, a security control is applied. The security control requires an additional officer to always verify the activities of check-in personnel. The cost value of 4 implies that it will cost more to employ additional staff to verify the activities of check-in personnel.

For Risk 2, the security requirement to reduce the risk is by educating airline passengers on possible phishing attack methods. To achieve this, a security control is applied by using only secured https websites for booking and passenger check-in. The cost value of 2 implies that it will cost less to educate the passengers against phishing methods and provide secured website for booking and check-in activities.

5.1.2 Luggage Information Risk Treatment

The following risks are identified in the asset luggage information –

Risk 3: Personnel records values lower than actual weight of luggage, and ground operations uses the information in the loading of the aircraft because luggage information which results to loss of integrity of luggage information and incorrect calculation of cg of the aircraft.

Risk 4: Personnel accepts luggage and adds contraband item to passenger’s luggage, sends luggage and luggage information to ground operations to load the aircraft because personnel activity is not monitored which results to loss of integrity of contents of passenger luggage and loss of trust in luggage check-in process.

Table 12: Luggage information risk treatment table

	Risk 3		Risk 4	
Risk treatment	Treatment cost	Risk reduction	Treatment cost	Risk reduction
Security requirement		Monitor activities of luggage check-in personnel.		Monitor activities of luggage check-in personnel.
Controls	2	Random checks to	1	Install camera to

		verify weight records with actual weight of luggage.		record luggage check-in personnel activities.
--	--	--	--	---

The security requirement for reducing Risk3 is by monitoring activities of luggage check-in personnel. The security control that must be implemented to achieve this is performing random checks on activities of luggage check-in personnel. The risk treatment value of 2 implies that less cost is required perform checks to verify data recorded by personnel.

For Risk 4, the security requirement is same as requirement for Risk 3 which is monitoring activities of personnel. However, a different security control is applied. The control is achieved by installing cameras to record activities of luggage check-in personnel. The treatment cost of 1 shows that not much money is required to mount security cameras to monitor activities of check-in personnel.

5.1.3 Fuelslip Risk Treatment

The following risks are identified in the asset fuelslip -

Risk 5: Malicious insider with access to computer that stores fuelslip make changes to the data contained in fuelslip before it is sent to service provider because the document is not encrypted which results to loss of integrity of fuelslip and can cause the aircraft to be loaded with wrong quantity and type of fuel.

Risk 6: Attacker intercepts fuelslip, changes data contained, sends to supplier, refueling is conducted based on information on fuelslip because messaging system can spoofed, which causes loss of integrity of fuelslip and can result in loading the aircraft with wrong quantity and type of fuel.

The table below shows security requirement and controls which must be applied to reduce Risk5 and Risk6.

Table 13. Fuelslip risk treatment.

	Risk5		Risk6	
Risk	Treatment	Risk reduction	Treatment	Risk reduction

treatment	cost		cost	
Security requirement		access control on fuelslip document		Make information contained in fuelslip unreadable.
Controls	4	encrypt fuelslip document	4	Verifies received document with previous originals received. (Blockchain cryptographic digest PKI or PGP) Encrypt fuelslip document

The security requirement for risk5 is by controlling access to the fuelslip document. Access control on fuelslip can be achieved by encrypting the fuelslip document. Such encryption that relies on Public Key Infrastructure (PKI) can be used in this case. The fuelslips and other documents that contain service requirements can be encrypted with private keys of the selected supplier and therefore only the supplier can view the document even when intercepted by another person.

For Risk6, the same security requirement and security control applied in Risk5 is also applied in Risk6. The risk treatment value of 4 in the risk5 and risk6 respectively implies that it will cost the airline a lot of money to implement encryption that uses PKI.

5.1.4 Cargo Assignment Risk Treatment

The following risks are identified in the asset cargo assignment -

Risk 7: Malicious insider with access to cargo assignment document make changes to cargo assignment document before it is sent to service provider because cargo assignment document is not encrypted which causes loss of integrity of cargo assignment and improper loading of the aircraft and can result to instability of the aircraft in the air.

Risk 8: *Attacker hacks airline mailing list, receives cargo assignment, changes data contained, sends to service provider, loading is conducted based on information in cargo assignment, because mailing list is not fully secured which causes loss of integrity of cargo assignment and can result to overloading the aircraft.*

The table below shows security requirement and necessary controls reduce Risk7 and Risk8 identified in cargo assignment document.

Table 14: Cargo assignment risk treatment

	Risk7		Risk8	
Risk treatment	Treatment cost	Risk reduction	Treatment cost	Risk reduction
Security requirement		Access control on cargo assignment document.		Make information contained in cargo assignment unreadable.
Controls	4	Encrypt cargo assignment document.	4	Verify received document with previous originals received. Encrypt cargo assignment document.

The security requirement and control for Risk7 and Risk8 are same. In order to reduce risks on cargo assignment document, access control must be implemented as a security requirement on cargo assignment document. Access control can be achieved by applying encryption that relies on PKI. As a result, only the service provider can have access to the document even when intercepted. The cost value of 4 implies that a lot of

money is required to implement encryption that depends on PKI in order to reduce the risks identified in risk7 and risk8.

5.2 Evaluation of Risks

This goal of this section is to evaluate how the security requirements and controls applied in the risk treatment tables affected the risks identified in the risk analysis. The Goal Question Metric (GQM) is applied in order to evaluate security requirements.

The GQM framework provides a top-down approach to measurement. The following questions are generated when GQM is applied in the context of ISSRM domain model [24].

- Maximization of risk reduction
- Minimization of risk treatment cost

In this analysis, our emphasis is on risk reduction estimation. The tables below show the risks identified and GQM questions for measuring the goals.

5.2.1 Maximizing Risk Reduction

The analysis performed in section 5.1 doesn't show how the security requirements and controls applied in the risk treatment tables reduced the risks identified. By applying the risk reduction metric questions, we can figure out the risk levels before applying security controls and risk levels after applying security controls. In this way we can estimate and quantify the effect of security controls on the risks identified in the analysis.

5.2.2 Risk Metrics and Calculations

The value for risk components for all the risk analysed above were gotten after interview with industry experts. The data are based on guesstimate as a result of the absence of literature reference.

The following risk components - business asset value, threat likelihood, vulnerability level, security objective are between the values of 0 to 5. The risk event, risk impact and risk level are calculated as below -

Risk event = threat likelihood + vulnerability level - 1 [45]

Impact = maximum value of the security criterion

Risk level = risk event x impact.

$$^1\text{Maximum risk} = (5 + 5 - 1) * 5 = 45$$

$$\text{Minimum risk} = (0 + 0 - 1) * 0 = 0$$

The minimum risk obtainable is 0, while the maximum risk obtainable is 45. Therefore, 0 and 45 represent the boundaries of the risks.

Metric A provides information about risk level when security control is not yet applied while Metric B provides information about risk level after security control is applied.

5.2.3 Risk 1 reduction metrics

Table 15. Risk 1 reduction metrics.

Goal	Maximize risk1 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?
Metric A	Risk level = 12	Risk Event potentiality = 4 Threat Likelihood = 2 Vulnerability level = 3	Impact level = 3 Security objective = 3 Business asset value=3	
Metric B	Risk level = 6	Risk Event potentiality = 1 Threat Likelihood = 1 Vulnerability level = 2	Impact level =3 Security objective = 3 Business asset value =3	Risk reduction level= 6

Metric A – Risk1 level before security controls

$$\text{Risk event} = \text{threat likelihood} + \text{vulnerability level} - 1$$

¹ The data used in risk metrics and calculations were gotten after several interviews with industrial experts

$$= 2 + 3 - 1$$

$$= 4$$

Impact = maximum value of the security criterion

$$= 3$$

Risk level = risk event x impact

$$= 4 * 3$$

$$= 12$$

Metric B – Risk1 level after security controls

Risk event = 2 + 1 - 1

$$= 2$$

Impact = 3

Risk level = 3 * 2

$$= 6$$

Risk reduction level = Risk level A – Risk level B

$$= 12 - 6$$

$$= 6$$

5.2.4 Risk 2 reduction metrics

Table 16. Risk 2 reduction metrics

Goal	Maximize Risk2 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?
Metric A	Risk level = 15	Risk Event potentiality = 5 Threat Likelihood = 4 Vulnerability level = 2	Impact level = 3 Security objective = 3 Business asset value=2	
Metric B	Risk level	Risk Event	Impact level = 3	Risk reduction

	= 9	potentiality =3 Threat Likelihood =3 Vulnerability level = 1	Security objective =3 Business asset value=3	level= 6
--	-----	--	---	----------

Metric A – Risk2 level before security controls

Risk event = threat likelihood + vulnerability level -1
= 4 + 2 -1
= 5

Impact = maximum value of the security criterion
= 3

Risk level = risk event x impact
= 5 * 3
= 15

Metric B – Risk 2 level after security controls

Risk event = 3 + 1 -1
= 3

Impact = 3

Risk level = 3* 3
= 9

Risk reduction level = Risk level A – Risk level B
= 15 – 9
= 6

5.2.5 Risk 3 reduction metrics

Table 17. Risk 3 reduction metrics.

Goal	Maximize risk3 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?

Metric	Risk level = 4	Risk Event potentiality = 2 Threat Likelihood = 2 Vulnerability level = 1	Impact level = 2 Security objective = 2 Business asset value=1	
	Risk level = 2	Risk Event potentiality=1 Threat Likelihood=1 Vulnerability level=1	Impact level = 2 Security objective =2 Business asset value=1	Risk reduction level= 2

Metric A – Risk3 level before security controls

Risk event = threat likelihood + vulnerability level -1

$$= 2 + 1 - 1$$

$$= 2$$

Impact = maximum value of the security criterion

$$= 2$$

Risk level = risk event x impact

$$= 2 * 2$$

$$= 4$$

Metric B – Risk3 level after security controls

Risk event = 1 + 1 - 1

$$= 1$$

Impact = 2

Risk level = 2 * 1

$$= 2$$

Risk reduction level = Risk level A – Risk level B

$$= 4 - 2$$

$$= 2$$

5.2.6 Risk 4 reduction metrics

Table 18: Risk 4 reduction metrics

Goal	Maximize risk4 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?
Metric A	Risk level = 15	Risk Event potentiality = 5 Threat Likelihood = 2 Vulnerability level = 4	Impact level = 3 Security objective = 3 Business asset value=2	
Metric B	Risk level = 6	Risk Event potentiality= 2 Threat Likelihood=1 Vulnerability level = 2	Impact level = 3 Security objective = 3 Business asset value=2	Risk reduction level= 9

Metric A – Risk4 level before security controls

Risk event = threat likelihood + vulnerability level -1

$$= 2 + 4 - 1$$

$$= 5$$

Impact = maximum value of the security criterion

$$= 3$$

Risk level = risk event x impact

$$= 5 * 3$$

$$= 15$$

Metric B – Risk4 level after security controls

Risk event = 2 + 1 - 1

$$= 2$$

Impact = 3

Risk level = 2 * 3

$$= 6$$

Risk reduction level = Risk level A – Risk level B

$$= 15 - 6$$

5.2.7 Risk 5 reduction metrics

Table 19. Risk 5 reduction metrics.

Goal	Maximize risk5 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?
Metric A	Risk level = 20	Risk Event potentiality =5 Threat Likelihood = 3 Vulnerability level=3	Impact level = 4 Security objective = 4 Business asset value=3	
Metric B	Risk level = 4	Risk Event potentiality = 1 Threat Likelihood = 1 Vulnerability level=1	Impact level = 4 Security objective =4 Business asset value=3	Risk reduction level= 16

Metric A – Risk5 level before security controls

Risk event = threat likelihood + vulnerability level -1
 = 3 + 3 -1
 = 5

Impact = maximum value of the security criterion
 = 4

Risk level = risk event x impact
 = 5 * 4
 = 16

Metric B – Risk5 level after security controls

$$\begin{aligned} \text{Risk event} &= 1 + 1 - 1 \\ &= 1 \end{aligned}$$

$$\text{Impact} = 4$$

$$\begin{aligned} \text{Risk level} &= 4 * 1 \\ &= 4 \end{aligned}$$

$$\begin{aligned} \text{Risk reduction level} &= \text{Risk level A} - \text{Risk level B} \\ &= 20 - 4 \\ &= 16 \end{aligned}$$

5.2.8 Risk 6 reduction metrics

Table 20: Risk 6 reduction metrics

Goal	Maximize risk6 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?
Metric A	Risk level = 16	Risk Event potentiality = 4 Threat Likelihood = 2 Vulnerability level = 3	Impact level = 4 Security objective = 4 Business asset value=3	
Metric B	Risk level = 4	Risk Event potentiality = 1 Threat Likelihood = 1 Vulnerability level = 1	Impact level = 4 Security objective = 4 Business asset value=3	Risk reduction level= 12

Metric A – Risk6 level before security controls

$$\text{Risk event} = \text{threat likelihood} + \text{vulnerability level} - 1$$

$$= 2 + 3 - 1$$

$$= 2$$

Impact = maximum value of the security criterion

$$= 4$$

Risk level = risk event x impact

$$= 4 * 4$$

$$= 16$$

Metric B – Risk6 level after security controls

Risk event = $1 + 1 - 1$

$$= 1$$

Impact = 4

Risk level = $4 * 1$

$$= 4$$

Risk reduction level = Risk level A – Risk level B

$$= 16 - 4$$

$$= 12$$

5.2.9 Risk 7 reduction metrics

Table 21. Risk 7 reduction metrics.

Goal	Maximize risk7 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?
Metric A	Risk level = 12	Risk Event potentiality = 4 Threat Likelihood = 3 Vulnerability level = 2	Impact level = 3 Security objective = 3 Business asset value = 1	
Metric B	Risk Level = 3	Risk Event potentiality = 1	Impact Level = 3 Security Objective = 3	Risk reduction

		Threat Likelihood =1 Vulnerability level=1	Business asset value=1	level= 9
--	--	---	---------------------------	----------

Metric A – Risk7 level before security control

Risk event = threat likelihood + vulnerability level -1
= 3 + 2 -1
= 4

Impact = maximum value of the security criterion
= 3

Risk level = risk event x impact
= 4 * 3
= 12

Metric B – Risk7 level after security controls

Risk event = 1+ 1 - 1
= 1

Impact = 3

Risk level = 3 * 1
= 3

Risk reduction level = Risk level A – Risk level B
= 12 - 3
= 9

5.2.10 Risk 8 reduction metrics

Table 22: Risk 8 reduction metrics

Goal	Maximize risk8 reduction			
Question	What is the risk level?	What is the occurrence frequency?	What is the importance regarding the business?	What is the risk reduction level after treatment of risk?

Metric A	Risk level = 9	Risk Event potentiality = 3 Threat Likelihood = 2 Vulnerability level= 2	Impact level = 3 Security objective = 3 Business asset value = 1	
Metric B	Risk Level= 6	Risk Event potentiality = 2 Threat Likelihood = 2 Vulnerability level=1	Impact level = Security objective = 3 Business asset value=1	Risk reduction level=3

Metric A – Risk8 level before security controls

$$\begin{aligned} \text{Risk event} &= \text{threat likelihood} + \text{vulnerability level} - 1 \\ &= 2 + 2 - 1 \\ &= 3 \end{aligned}$$

$$\begin{aligned} \text{Impact} &= \text{maximum value of the security criterion} \\ &= 3 \end{aligned}$$

$$\begin{aligned} \text{Risk level} &= \text{risk event} \times \text{impact} \\ &= 3 * 3 \\ &= 9 \end{aligned}$$

Metric B – Risk8 level after security controls

$$\begin{aligned} \text{Risk event} &= 2 + 1 - 1 \\ &= 2 \end{aligned}$$

$$\text{Impact} = 3$$

$$\begin{aligned} \text{Risk level} &= 3 * 2 \\ &= 6 \end{aligned}$$

$$\begin{aligned} \text{Risk reduction level} &= \text{Risk level A} - \text{Risk level B} \\ &= 9 - 6 \\ &= 3 \end{aligned}$$

5.3 Analyses of Risk Metrics

Due to availability of meager resources to provide counter measures for all the risks identified, it necessary that the risks are prioritized. The priority is determined by performing trade-off analyses based on the value of the assets, risk treatment cost and risk reduction level [45].

Table23: Risk metrics before and after risk treatment

	Before treatment					After treatment				Risk reduction level	Business asset value	Cost of counter-measure
	Vulnerability level	Threat likelihood	Event potentiality	Impact level	Risk level1	Vulnerability level	Threat likelihood	Event potentiality	Risk level2			
Risk1	3	2	4	3	12	2	1	2	6	6	3	4
Risk2	2	4	5	3	15	1	3	3	9	6	3	2
Risk3	1	2	2	2	4	1	1	1	2	2	1	2
Risk4	4	2	5	3	15	2	1	2	6	9	1	1
Risk5	3	3	5	4	20	1	1	1	4	16	3	4
Risk6	3	2	4	4	16	1	1	1	4	12	3	4
Risk7	2	3	4	3	12	1	1	1	4	8	1	4
Risk8	2	2	3	3	9	1	2	2	6	3	1	4

The table above shows risk metrics before risk treatment and after treatment, risk reduction level, business asset value and cost of treatment. From the table, the following graphs – RRL-value, RRL-cost, and cost-value are generated. The graphs are divided into four quadrants and priority on each quadrant is identified by labeling Low (L), Medium (M) and High (H) on each quadrant.

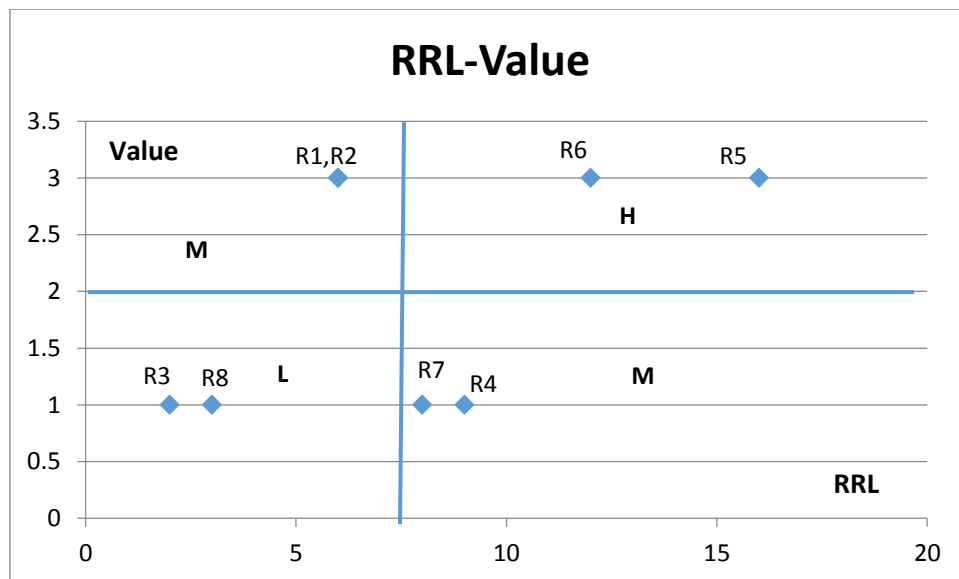


Figure 9: graph1

The figure above shows a graph of risk reduction level against business asset value. The desire scenario is a high value asset with a high risk reduction level. This can be identified in the quadrant that has R6, R5 and therefore represent a high priority for this this graph. The medium priorities quadrants have high assets value with low risk reduction level and low valued assets with high risk reduction values. These situations are found in quadrants that have R1, R2 and R7, R4 respectively. The least desired

situation is a low valued asset with a low risk reduction and this is found in quadrant that has R3 and R8.

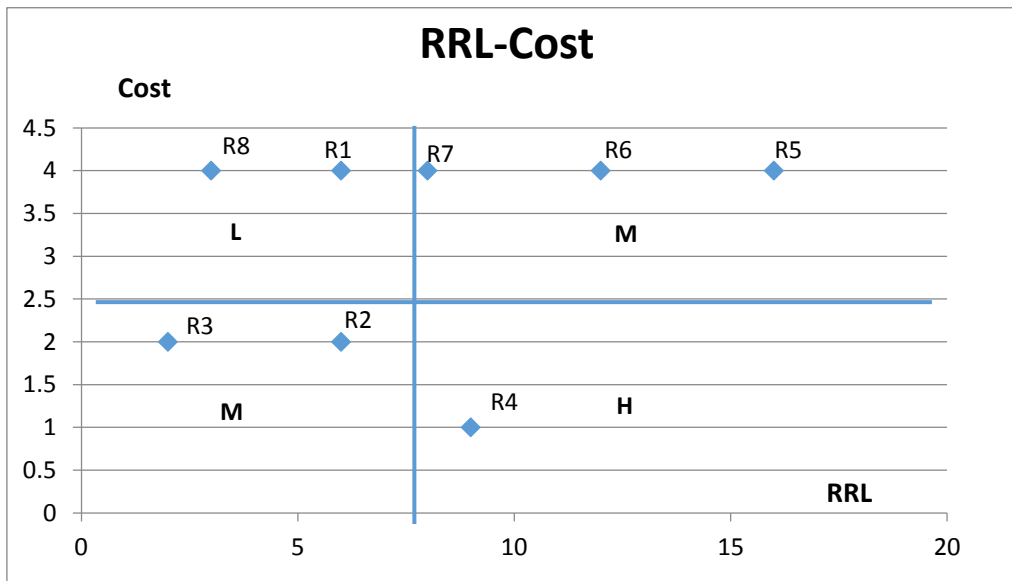


Figure 10: graph2

The figure above shows a graph of risk reduction level against cost of counter measure. The ideal situation is a low cost value with a high risk reduction value. This can be identified in the quadrant that has R4 and therefore represent a high priority for this this graph. The medium priorities quadrants have high cost value with high risk reduction level and low cost with low risk reduction values. These situations are found in quadrants that have R5, R6, R7 and R2, R3 respectively. The low priority can be identified in quadrant that has high cost and low risk reduction. This quadrant contains R1 and R8.

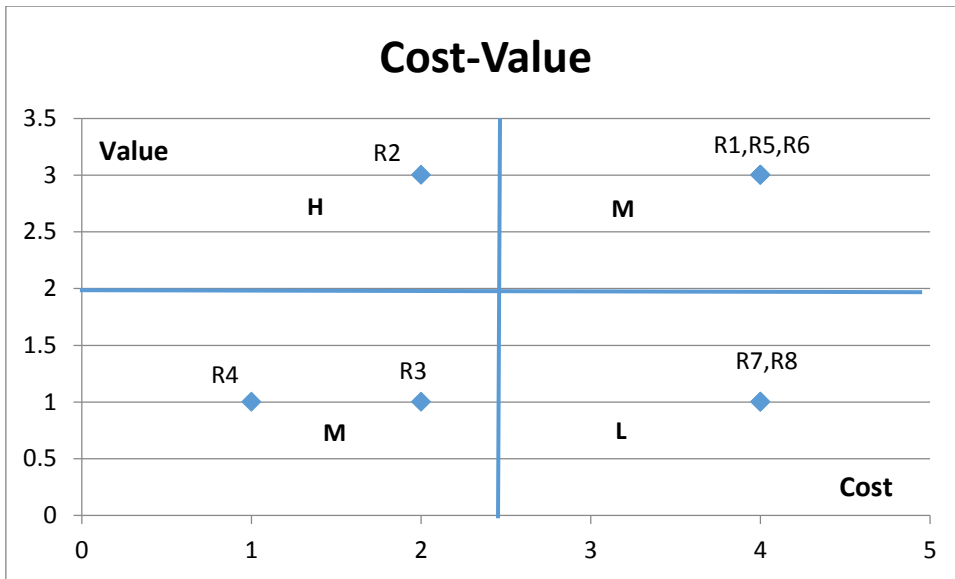


Figure11: graph3

The figure above is a graph of cost of counter measure against business asset value. A low cost treatment with a high valued asset represents a high priority and can be seen in quadrant that has R2. The medium priority are found in quadrants that have high valued assets with high cost of counter measure and low valued assets and low cost of counter measure. These are found in the quadrant that has R1, R5, R6 and the quadrant that has R3, R4. The least ideal situation is a low valued asset with a high cost of risk treatment and it is found in quadrant that has R7, R8.

Table 24: Risk Priority Table

	Value-RRL	RRL-cost	value-cost		
	Graph 1	Graph 2	Graph 3		
Risk1	2	1	2	5	Medium priority
Risk2	2	2	3	7	High priority
Risk3	1	2	2	5	Medium priority
Risk4	2	3	2	7	High priority
Risk5	3	2	2	7	High priority
Risk6	3	2	2	7	High priority
Risk7	2	2	1	5	Medium priority
Risk8	1	1	1	3	Low priority

The table shows risk priority derived by combining graph 1, graph2 and graph3. A value of 1 is assigned to low priority risks, medium priority risks has a value of 2, while the value of 3 is assigned to high priority risks. By the adding these values across the three

graphs, a priority which depends on value of business asset, cost of countermeasure and risk reduction level can be estimated.

From the table, the risks with high priorities are Risk2, Risk4, Risk5 and Risk6. The medium priority risks are R1, R3 and R7. The least priority risk is Risk8.

5.4 Conclusion

This chapter is made up of two sections, risk treatment and risk evaluation respectively. In the risk treatment section, security requirement and controls were applied on risks identified in section 4.0. The purpose of the controls applied is to reduce the risks to a considerable level.

The risk reduction achieved after introducing security controls is determined by making estimated calculations. This was done by first calculating the risk levels before security controls were applied and after security control were applied. In the tables in this chapter, Metric A rows are GQM values before security controls and Metric B rows are values after security controls were applied. The risk reduction level was calculated from the two risk levels represented by Metric A and Metric B.

Finally, analysis was also performed to determine the priority of risks identified. The estimation of risk priorities is based on value of asset involved, cost of risk treatment and risk reduction level achieved after applying counter measure.

6 Risk Simulation

The objective of this chapter is to simulate one of the risks outlined in section 5.1. The simulated risk is chosen based on the risk priority identified in table 23. The risk with the highest priority is chosen for simulation. The goal of the simulation is to demonstrate how attack on airline turnaround operations can be carried out by exploiting one of the identified risks. The simulation also shows the success of the attack before application of security controls and after application of security controls. The effects of the attack on the airline resources are also observed.

The chapter starts by describing the risk and how the attack can be carried out by exploiting the weakness posed by the identified risk. In the second part of the chapter, a platform independent simulation models is used to describe the attack simulation. The final part of the chapter involves using Anylogic simulation toolkit in building the computer based simulation and analyses of the simulation result.

6.1 Description of Risk

From the table 23, Risk 4 which is among the risks with the highest priority is chosen for the simulation purpose. Also, risk 4 involves exchange of service requirement between airline and service provider using the messaging system. This risk can easily be represented in a computer based environment for simulation purposes.

Risk 4 - *“An attacker intercepts fuelslip, changes data contained, sends to supplier, refueling is conducted based on information on fuelslip because messaging system can spoofed, which causes loss of integrity of fuelslip and can result in loading the aircraft with wrong quantity and type of fuel”*.

The risk above identified in the *fuelslip* business asset is capable of causing physical damage to the aircraft and putting the life of passengers at risk, according to [35] and [36]. The attack identified in the risk is the *interception and changing of data contained in the fuelslip*. The detail of how this attack can be carried out is explained below.

6.1.1 Interception of airline fuelslip over messaging system

There are many ways an attacker can intercept service requirement sent by the airline to the service provider. For the sake of space and scope of this thesis, two methods of carrying out this attack are described. These methods are - Attacking airline mailing list and DNS poisoning attack.

6.1.1.1 Mailing list attack

Organizations have address-books and mailing lists that contain details such as email addresses of their service providers and suppliers. Service requests and requirements are usually over email from clients to service providers. From Figure 8, it is shown that service requirements for refueling of aircraft are contained in the fuelslip and the fuelslip are sent to the service provider through the messaging system. The fuelslip contains information such as quantity and fuel type is sent to the supplier through the messaging system.

A malicious insider with access to the server that contains the airline's address book can modify the mailing list. For the purpose of simulation of this attack, malicious insider replaces the fuel supplier email address with that of an attacker. The airline, instead of sending fuelslip to the service provider sends it to the attacker.

The attacker on receiving the fuelslip modifies the service requirements contained in the fuelslip. The attacker can reduce the quantity of fuel or change the type of fuel to be loaded on the aircraft. After modifying the service requirement contained in the fuelslip document, attacker forwards it to the service provider.

The service provider performs aircraft refueling operation based on service requirements outlined in fuelslip. As a result, the aircraft is loaded with insufficient fuel or with the wrong type of fuel. According to [35] and [36], loading the aircraft with the wrong quantity of fuel or wrong type of fuel results in air crashes.

6.1.1.2 DNS Poisoning attack

This attack is similar to the one described in the mailing list attack. However, the difference is that in DNS poisoning attack, a malicious insider will modify the ip address in the DNS and email is delivered to a rogue receiver [27]. The weakness in the mailing list attack is that the airline agent can view the email address of the service

provider before sending. There is a possibility of observing the changes made in supplier email address, thereby making the attack unsuccessful.

In order to describe the DNS poisoning attack, it is necessary to understand how email messaging system works. A brief summary describing how email messaging works is shown below¹.

- *A sender composes an email containing the following: address of receiver, subject and body of message.*
- *Simple mail transfer protocol (SMTP) server verifies the email header and identifies the domain name in address of the receiver.*
- *SMTP server through the DNS server resolves the domain name of the receiver to an IP address.*
- *SMTP server forwards the email to the mail server of the IP address.*

A malicious insider that has access to the DNS server can make changes to information contained in the DNS system and thereby divert an email to a malicious attacker [27]. It is possible that an insider changes the IP address of the supplier's domain to that of the attacker. When an email is sent to supplier from the airline, SMTP server delivers the email to the attacker's email server. The attacker receives the email, make changes to the service requirements in the fuelslip and forward to the service provider.

Transport layer security (TLS) based email encryption which is used by Google and some other email clients cannot prevent this attack. TLS works by encrypting sessions of emails as it transmitted over SMTP servers but the actual content of the email is not encrypted [42].

6.2 Platform independent simulation models

Models are used in simplifying and representing complex systems. The attack described above is a complex system because of number of agents involved and interactions that take place among these agents. For the purpose of simulation, the models described in the viewpoint framework are used in simplifying and modeling the attack. The

¹ A summary of graphical description of how email works from - <https://www.visiondesign.com/how-does-email-work-a-simple-illustrated-explanation/> accessed 28/11/2016

following models - goal model, role model, agent model, interaction model, knowledge model and behavioural model are used for this purpose.

6.2.1 Goal Model

A goal model is a representation of functional requirement of a system (simulation) [30]. From the description of the attack in section 6.1, the goal of the simulation is to attack the airline refueling process. To achieve this, the goal is broken down into three sub-goals - intercept fuelslip, change service requirement contained in fuelslip and conduct refueling with the new service requirement. The role which is necessary in achieving is attached to the specific goal.

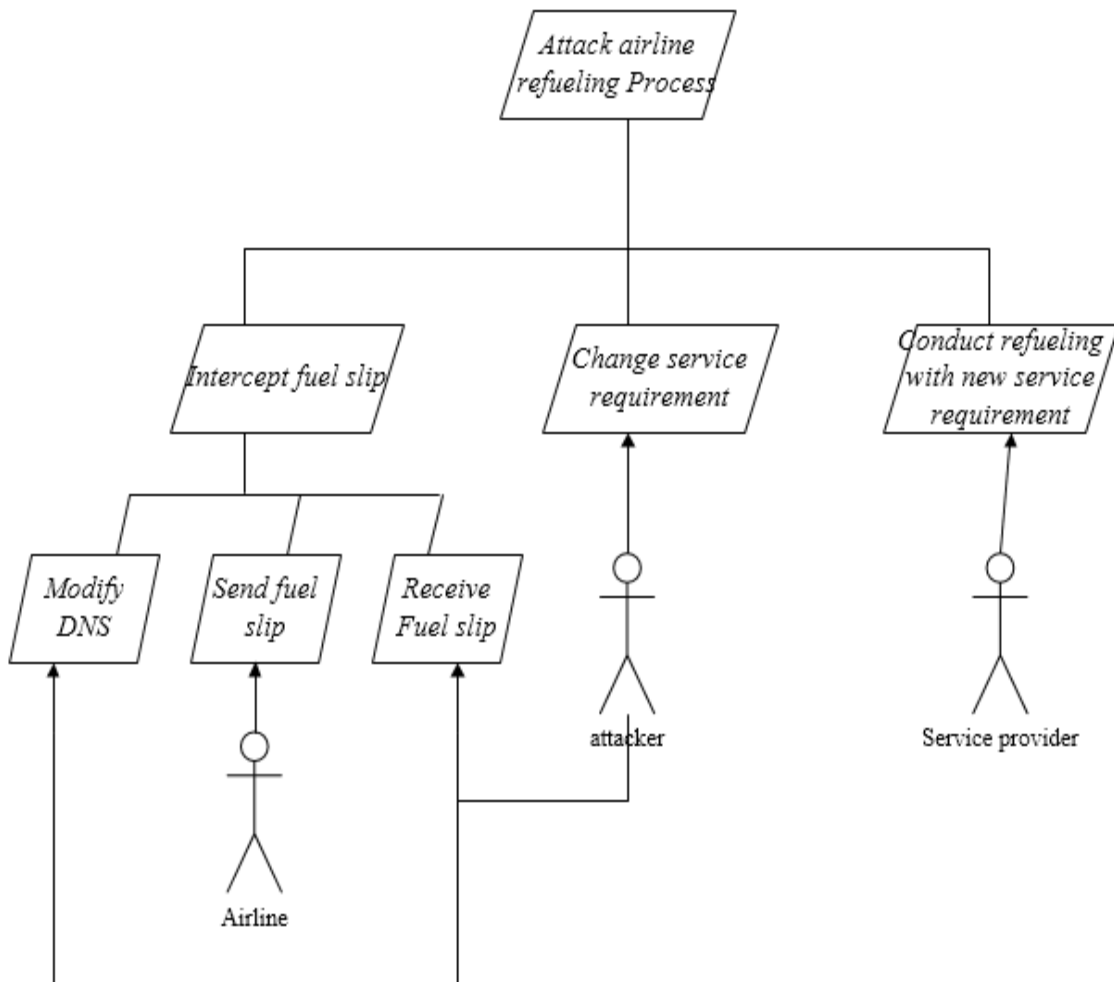


Figure 12: Risk simulation goal model

6.2.2 Role model: the following roles are identified in the risk simulation - airline, attacker and service provider. The table below describes the roles identified in the attack simulation and constraint on each of the roles.

Table 25. Risk simulation role model

Role name	Description of role	Constraint
Airline	<ul style="list-style-type: none"> • Prepares fuelslip • Sends fuelslip to service provider 	Messages are sent to the service provider through the airline messaging system.
Attacker	<ul style="list-style-type: none"> • Hacks the airline messaging system • Intercepts fuelslip sent by the airline to the service provider • Modifies fuelslip • Sends fuelslip to the service provider 	Needs an insider to hack the airline messaging system
Service provider	<ul style="list-style-type: none"> • Receives fuelslip • Conducts refueling of the aircraft 	Refueling is conducted based on information on the fuelslip

6.2.3 Agent model: the agent model maps the roles to agents [30]. The table 15 above shows specific role of each agent in the simulation. The role airline is mapped to an airline agent. Attacker is mapped to two agents - insider agent and attacker agent. Finally, the role service provider is mapped to a refuelling agent.

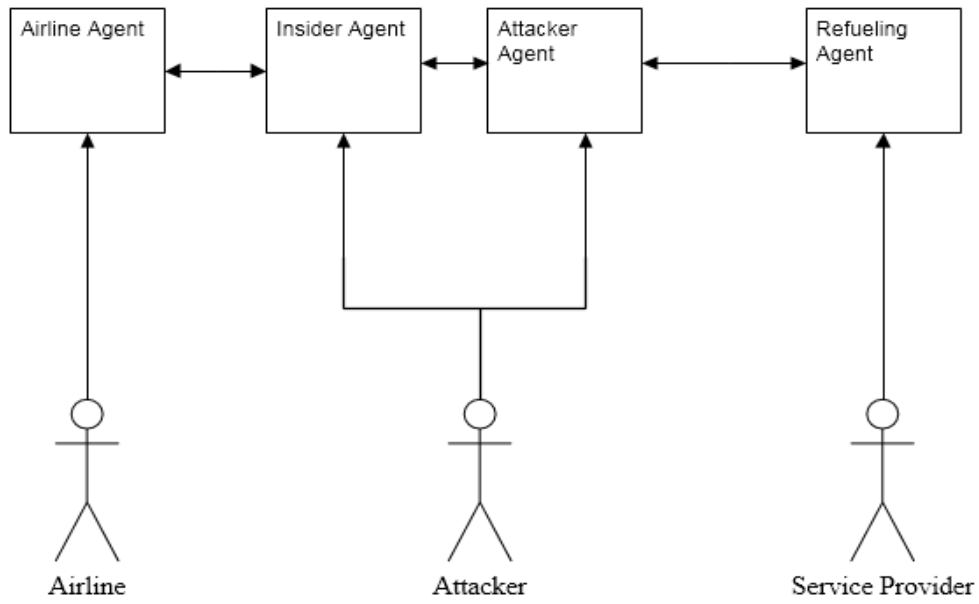


Figure 13. Risk simulation Agent Model

6.2.4 Interaction model: the interaction model outlines various interactions taking place among agents identified in the agent model.

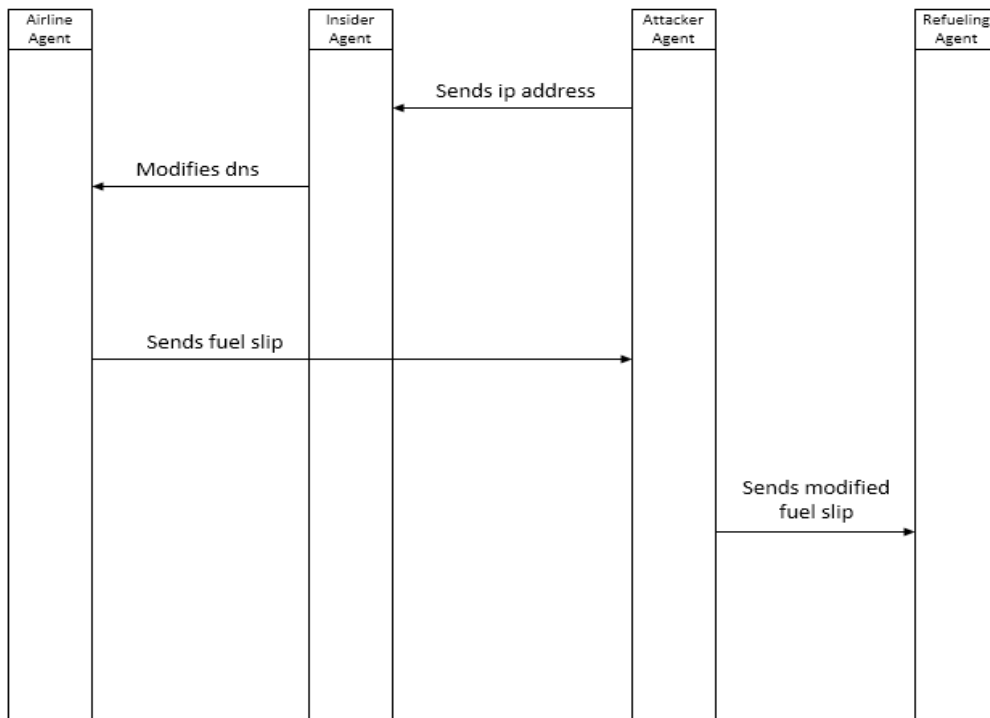


Figure 14. Risk Interaction Model

6.2.5 Knowledge Model

The knowledge model shows what information about the system is available to each agent. From the diagram below, information about the fuelslip is known by the following agents - Airline Agent, Attacker agent and Refueling Agent. The information contained in fuelslip can be represented as the quantity of fuel and type of fuel. Also, information of DNS is known by the attacker and insider agent. The information contained in DNS can be represented as the hostname and IP address.

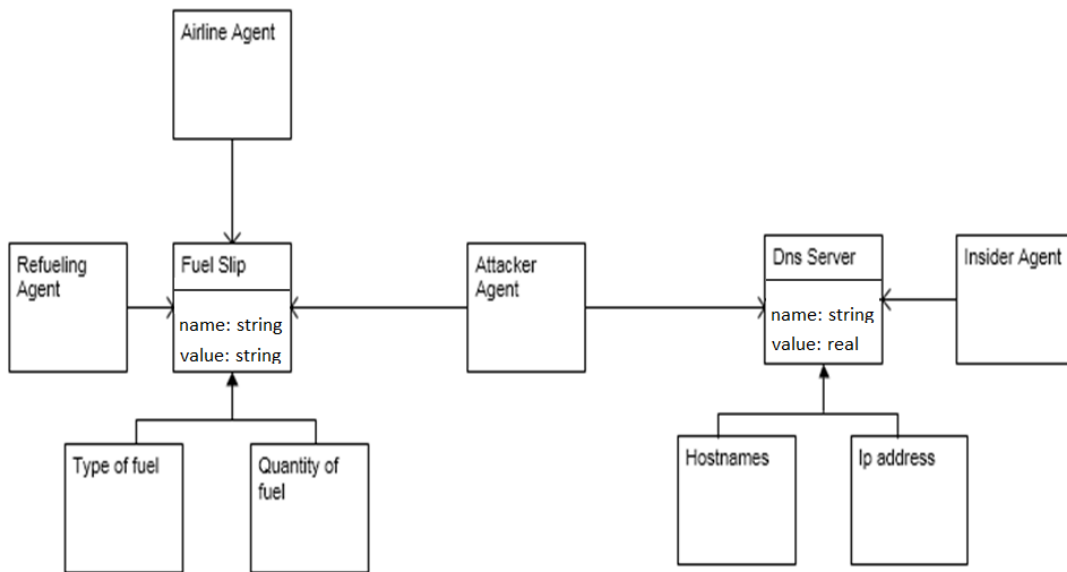


Figure 15. Risk simulation knowledge Model

6.2.6 Behavioural model

The behavioural model shows interactions that take place between an agent and other agents. The actions of the agent are outlined as well as the rules that determine such actions.

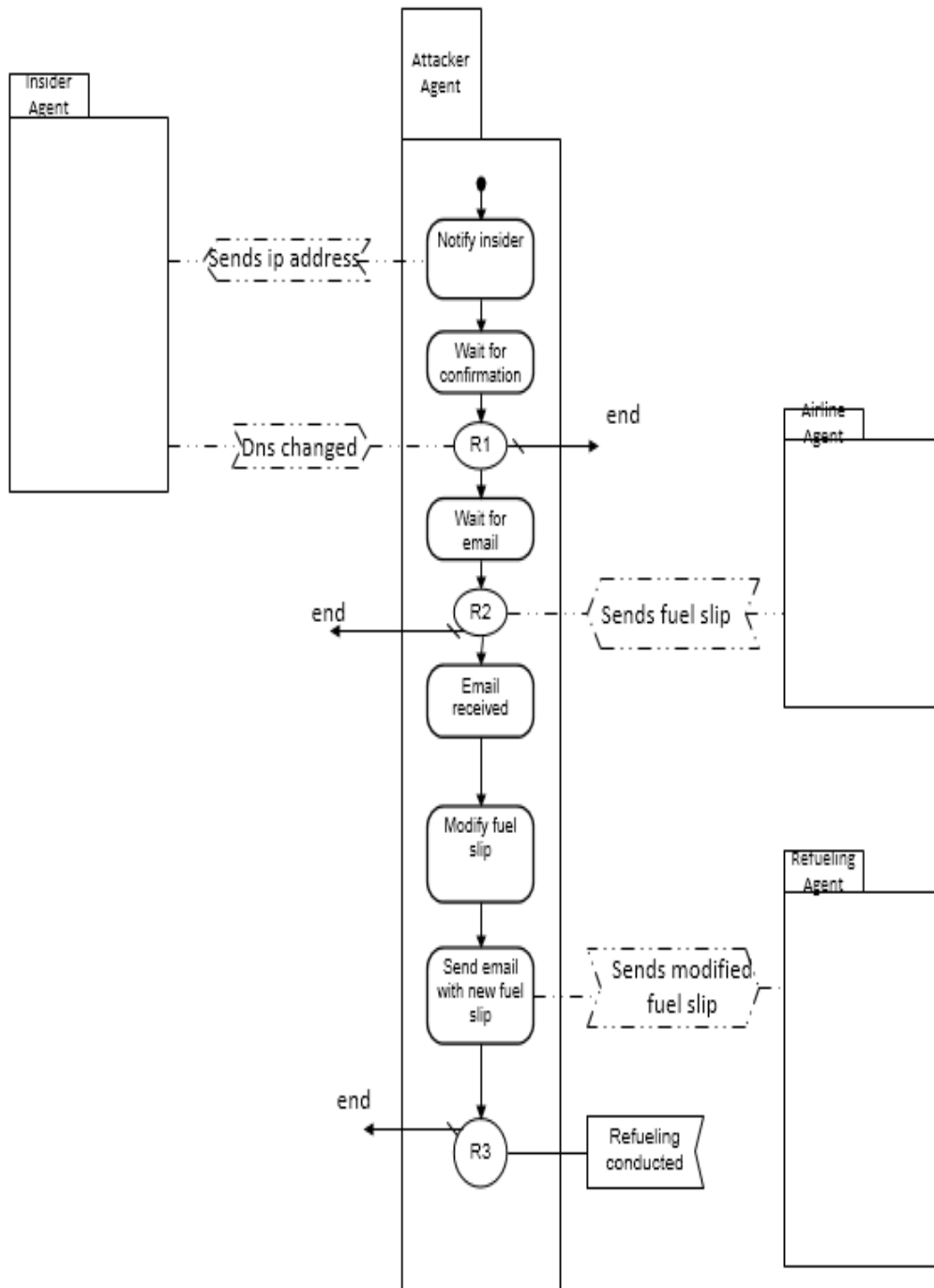


Figure 16. Risk behavioural model

The rules (R1, R2 and R3) represents 'what if' situations in the attack.

R1: If an insider agent is compromised (or bribed), what is the chances of successfully manipulating the DNS server?

R2: If the DNS has been successfully changed, what are the chances of attacker intercepting the fuelslip sent to service provider?

R3: If the service requirement has been changed, what are the chances of conducting refueling based on information in the modified fuelslip?


6.3 Anylogic Based Simulation

The computer based simulation in this section is carried out using Anylogic simulation toolkit (student edition). Anylogic provides process modelling blocks for modelling and describing discrete events. The Process Modelling is a collection of objects for defining process workflows and their associated resources [44]. The process modelling blocks are described in the table below.

6.3.1 Definition of Symbols

Table 26. Description of Anylogic Process Modelling Blocks [44]

Name	Picture	Description
Source		Generates agents. Is usually a starting point of a process model.
Sink		Disposes agents. Is usually an end point in a process model.
Delay		Delays agents for a given amount of time. The delay time is evaluated dynamically, may be stochastic and may depend on the agent as well as on any other conditions.
Seize		Seizes a given number of resource units from a given ResourcePool .
Release		Releases a given number of resource units previously seized by Seize object.
Service		Seizes a given number of resource units, delays the agent, and releases the seized units.
Exit		Takes the incoming agents out of the process flow and lets the user to specify what to do with them.
Resource pool		Defines a set of resource units that can be seized and released by agents using Seize , Release , Assembler and Service flowchart blocks.
Queue		A queue (a buffer) of agents waiting to be accepted by the next object(s) in the process flow, or a general-purpose storage for the agents.

Select		Routes the incoming agents to one of the two output ports depending on (probabilistic or deterministic) condition.
--------	---	--

6.3.2 Airline refuel attack Simulation

The figures [14] and [15] show screenshots of the simulation conducted using Anylogic simulation toolkit. The processes shown in the figures are described below of each of the figures.

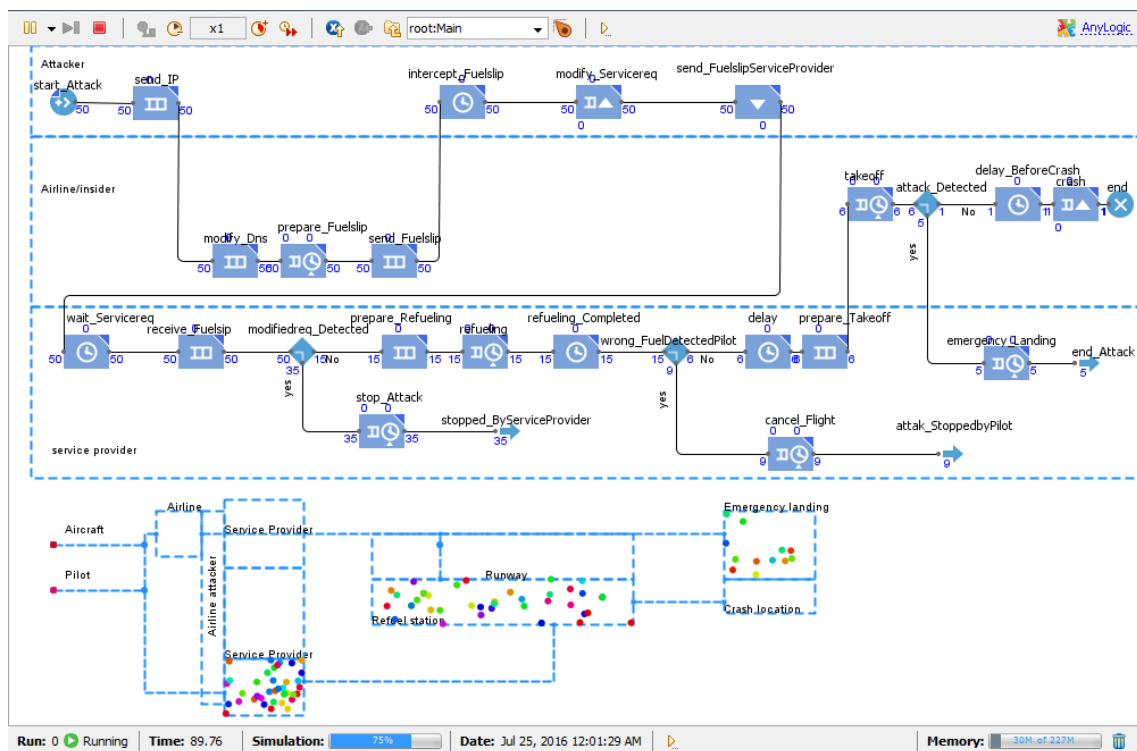


Figure 17. Airline Refuel Attack before Application of Security Controls

Process Description:

- Start_Attack: Attacker starts the attack process.*
- Send_IP: Attacker sends his IP details to an insider agent.*
- Modify_Dns: Insider agent modifies DNS with attacker's IP details.*
- Prepare_Fuelslip: Airline prepares fuelslip.*
- Send_Fuelslip: Airline sends fuelslip to service provider.*
- Intercept_Fuelslip: Attacker intercepts fuelslip.*
- Modify_Servicereq: Attacker modifies service requirement in fuelslip.*
- Send_FuelServiceProvider: Attacker sends modified fuelslip to service provider.*
- Wait_Servicereq: Service provider waits for refuelling service requirement.*

Receive_Fuelslip: Service provider receives fuelslip.
Modifyreq_Detected: Chances that service provider detects changes in fuelslip.
Stop_Attack: Service provider prepares to stop attack.
Stopped_ByServiceProvider: Process exit's as attacked is stopped by Service provider.
Prepare-Refueling: Service prepares aircraft for refuelling.
Refueling: Refuelling process by service provider.
Refueling_Completed: Refuelling is completed.
Wrong_FuelDetectedPilot: Pilot detects wrong fuel in the aircraft.
Cancel_Flight: Pilot cancels flight.
Attack_StoppedbyPilot: Attack is stopped by pilot.
Delay: delay before takeoff.
Prepare_takeoff: Pilot prepares for takeoff.
Takeoff: aircraft takeoff.
Attack_Detected:Probability that pilot detects abnormality on the aircraft.
Emergency_Landing: emergency landing due to detected abnormality.
End_Attack: Attack ends.
Delay_BeforeCrash: aircraft flies with wrong fuel in the tank.
Crash: flying with wrong fuel results in aircrash.

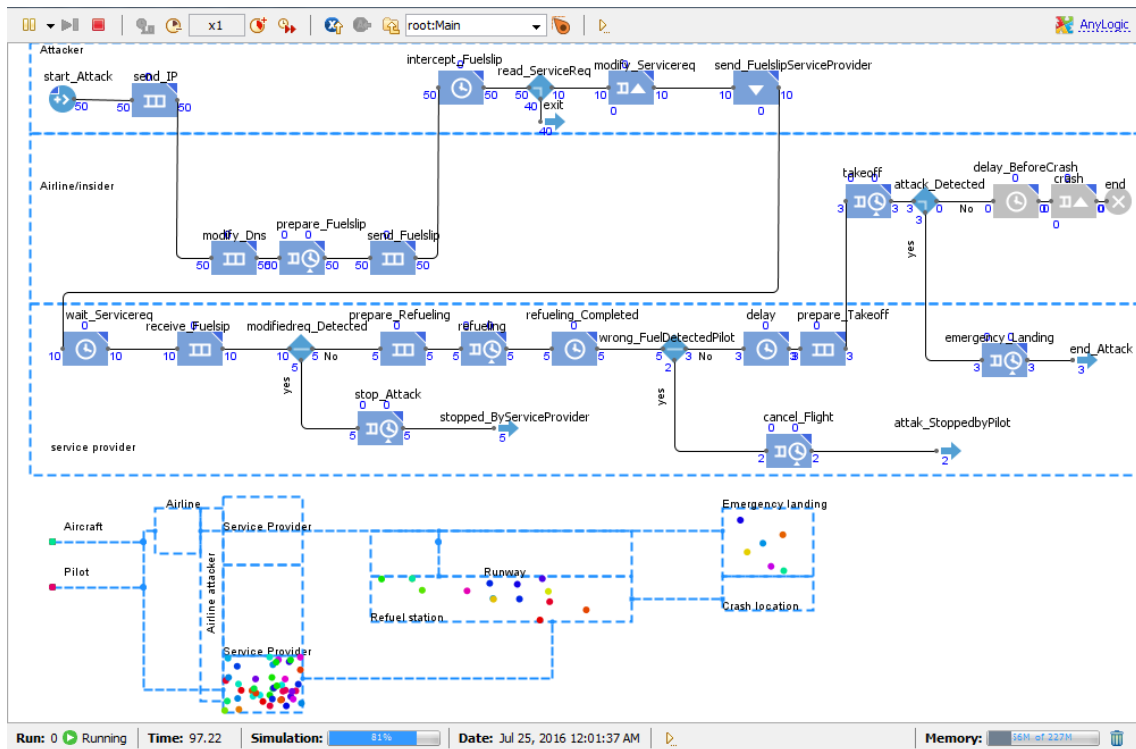


Figure 18. After Application of Security Controls

Process Description:

- Start_Attack: Attacker starts the attack process.*
- Send_IP: Attacker sends his IP details to an insider agent.*
- Modify_Dns: Insider agent modifies DNS with attacker’s IP details.*
- Prepare_Fuelslip: Airline prepares fuelslip.*
- Send_Fuelslip: Airline sends fuelslip to service provider.*
- Intercept_Fuelslip: Attacker intercepts fuelslip.*
- Read_Service: Probability that the attacker can decrypt encrypted fuelslip.*
- Exit: attack ends as attacker view fuelslip content.*
- Modify_Servicereq: Attacker modifies service requirement in fuelslip.*
- Send_FuelServiceProvider: Attacker sends modified fuelslip to service provider.*
- Wait_Servicereq: Service provider waits for refuelling service requirement.*
- Receive_Fuelslip: Service provider receives fuelslip.*
- Modifyreq_Detected: Chances that service provider detects changes in fuelslip.*
- Stop_Attack: Service provider prepares to stop attack.*
- Attack_StoppedbyServiceProvider: Process exit’s as attacked is stopped by Service provider.*
- Prepare-Refueling: Service prepares aircraft for refuelling.*
- Refueling: Refuelling process by service provider.*
- Refueling_Completed: Refuelling is completed.*
- Wrong_FuelDetectedPilot: Pilot detects wrong fuel in the aircraft.*
- Cancel_Flight: Pilot cancels flight.*
- Attack_StoppedbyPilot: Attack is stopped by pilot.*
- Delay: delay before takeoff.*
- Prepare_takeoff: Pilot prepares for takeoff.*
- Takeoff: aircraft takeoff.*
- Attack_Detected:Probability that pilot detects abnormality on the aircraft.*
- Emergency_Landing: emergency landing due to detected abnormality.*
- End_Attack: Attack ends.*
- Delay_BeforeCrash: aircraft flies with wrong fuel in the tank.*
- Crash: aircraft crashes and attack comes to an end.*

6.3.3 Analyses of Simulation Result

Table 27. Airline refuelling simulation result

Airline Refuel Attack	Before Security Control		After Security Control	
Total number of attempts	50	100%	50	100%
Attack stopped by Encryption	-	-	40	80
Attack stopped by Service Provider	35	70	5	10

Attack stopped by Pilot	9	18	2	4
Attack ends in emergency landing	5	10	3	6
Attack ends in air crash	1	2	0	0

The above table shows the end result of the attack after a specific number of attempts in percentage. Before security control was applied, 70% was stopped by service provider after detecting changes in fuelslip. The pilot stopped 18% of the attack after detecting wrong fuel during the refuelling process. About 12% of the attack is capable of causing physical damage to aircraft and possibly loss of life of the passengers; where 10% resulted in emergency landing and 2% leads to air crash.

After application of security controls, 80% of the attack was stopped due to encryption of fuelslip. The service provider stopped about 10% of the attack and 4% was stopped by the pilot. Only 6% of the attack could cause physical damage on the aircraft as a result of emergency landing.

Table 28. Effect of attack on Airline resources

Resources	Stopped by Service Provider	Stopped by Pilot	Emergency Landing	Air crash	Stopped by Encryption
Fuelslip	*	*	*	*	-
Pilot	-	*	*	*	-
Aircraft	-	*	*	*	-
Runway	-	-	*	*	-
Control Tower	-	-	*	*	-
Fire Service	-	-	*	*	-

The table above shows airline resources that are affected by various endings of the attack simulation. If the attack is stopped the service provider, the only resources affected is the fuelslip. This could have little economic damage on the airline as a result of delay experienced by the airline in using alternative means to deliver the refuelling service requirement to service provider.

If the attack is stopped by pilot, the following resources fuelslip, pilot, and aircraft are affected by the attack. This could cause enormous amount of economic loss resulting from waiting time in emptying and refuelling the aircraft with the proper fuel. In

addition, economic loss in finding alternative means of sending service requirements since messaging system is compromised.

Attack ending in emergency landing may cause physical damage to the aircraft, pilot (and passengers as well). Other resources belonging to the airport such as runway, fire service and control tower are also affected by the attack. This results in huge economic loss not only to the airline but also to the airport as well.

Attack ending aircrash is the worst situation envisaged which results in total destruction of the aircraft, loss of human life and tremendous loss to the airline.

When security control is applied and attack is ended as a result of encryption, no airline resources are affected and no economic loss resulting from the attack. This is best situation anticipated, the refuelling process executes perfectly with no hitches.

Therefore, if the fuelslip is not encrypted and the attack starts to execute, there must be negative consequence on the airline irrespective of how the attack ends. This is as a result of seized airline (and airport) resources, delays experienced, damages on the aircraft and possibly loss of human lives.

6.4 Conclusion

The simulation is performed to demonstrate the risk identified in the analysis section of this thesis. It also shows how the security requirements and controls reduced the risks. For the purpose of simulation, the risk which has the highest impact is chosen for simulation.

The simulation part of this work starts by describing the risk and how the attack identified in the risk can be carried out. In order to simplify the complexity in building the simulation, the viewpoint framework was used in developing models for the attack described. The simulation is divided into two, simulation of risk before application of security control and simulation of risk after application of security control.

By noting and comparing the numerical ends of the two simulations performed, the impact of the applied security control is determined. The airlines resources are linked to various ends of the simulation. The impact of security control on airline resources is determined by comparing various endings of the simulation and resources attached to them.

7 Conclusions

The final chapter of this thesis presents a summary of the research carried out in this work. Section 7.1 provide general conclusions, section 7.2 provides answers to all research questions for this work. The last section of this chapter 7.3 presents discussions arising from this work and areas of future work.

7.1 General conclusions

In this master thesis, security issues that affect enterprise collaborations are analysed using aviation sector as a case study. The airline turnaround workflow presents a good environment for this work because of the resource intensiveness of the operations and the processes involved are not part of the core competence of the airlines.

The end result of the analysis performed in this work is a security requirement and controls for managing risks resulting from collaboration between airlines and service providers. Though these security requirements and controls do not completely eliminate the security risks, evaluations performed this work show the risks were significantly reduced.

The analyses are based on processes in the airline turnaround workflow. This is because the turnaround operations present more opportunity for collaboration between airlines and service providers in airlines day of operations. The processes identified for analysis are Passenger management and Ground operations of the turnaround workflow. Assets involved in these processes are identified and grouped into business assets and information systems assets.

7.2 Answer to research questions

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

RQ1: How to identify relevant assets in enterprise collaborations that need to be secured?

The relevant assets involved collaborations between enterprises are identified by describing and modelling airline day of operations business processes. The turnaround workflow is used as an example of airline day of operation. A BPMN model describing

the airline turnaround processes was shows areas of collaboration. The processes in the turnaround workflow include – passenger management, ground operations and gate agent.

The research question presented can be answered more specifically by providing answers to the resulting what questions.

RQ1.1: What IT Systems are involved in these collaborations?

The IT systems involved in enterprise collaborations in the airline turnaround workflow can be described as the Information System (IS) assets. These IS assets supports the collaboration between the airline and service providers in the turnaround workflow.

The IS assets are listed below according the processes that make up the turnaround workflow.

The following IS assets are identified in passenger management process of airline turnaround - passenger Check-in process, luggage check-in process and passenger management pool.

The IS assets are available in ground operations are - messaging system, ground operations.

RQ1.2: What information is exchanged between collaborating systems?

The information exchanged between the collaborating systems are contained in the business assets exchanged between the airline and service provider in the turnaround workflow. The data that are contained in checked-in Passenger information are exchanged between collaborating systems are - personal details such as - name, address, contacts. Booking details such as - checked-in time, seat reservations.

The data contained in luggage information asset which are exchanged between collaborating systems are size of luggage, weight of luggage, content of luggage.

Information exchanged between collaborating systems in ground operations are as follows - type of fuel, quantity of fuel for fuelslip asset. For the cargo assignment, the information exchanged are checked-in cargo, weight of baggage and type of cargo.

RQ2: How do security risks threaten collaboration systems?

The risk components for the assets identified in RQ1.2 provide answers for this research questions.

RQ2.1: What are the threat agents?

The following threat agents are identified in passenger management process – a blacklisted passenger with a need to board the flight, an attacker that wants to sabotage the reputation of the airline by causing airline passengers to miss their flights, a luggage check-in personnel that wants to sabotage the safety of the flight by overloading the aircraft and luggage check-in personnel that wants to hide contraband item on passenger luggage.

The following threat agents are identified in ground operations - malicious insider that wants to sabotage the safety of the flight, an arbitrary attacker that wants to sabotage the safety of the flight.

RQ2.2: What are vulnerabilities?

- The following vulnerabilities are identified in assets in passenger management process - For passenger information assets, the vulnerabilities are check-in personnel could be bribed and passengers can't differentiate between original and fake check-in website.
- For luggage information asset, the vulnerabilities are luggage information generated by the check-in personnel is not verified and personnel activities are not monitored
- The following vulnerabilities are identified in assets in passenger ground Operations – For fuel-slip asset, the vulnerabilities are fuelslip document is not encrypted and email messages between airlines and service providers can be intercepted.
- For cargo assignment asset, the vulnerabilities cargo assignment document is not encrypted and mailing list is not fully secured.

RQ2.3: What are attack methods?

The attack methods for the assets identified in the passenger management process of airline turnaround workflow are as follows -

For checked-in passenger information asset

- Blacklisted passenger steals checked in passenger information, presents fake document, gets checked-in and

- An attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight.

For luggage information asset

- Personnel measures and records values lower than actual weight of luggage, sends luggage and luggage information to ground operations for onward loading on the aircraft.
- Personnel accepts luggage and adds contraband item to passengers' luggage, sends luggage and luggage information to ground operations to load the aircraft

The attack methods for the assets identified in the ground operations of airline turnaround workflow are as follows:

For the fuel-slip asset, the attack methods are –

- Malicious insider accesses the fuelslip document and changes the data contained in the document.
- Attacker intercepts fuelslip, receives fuelslip, changes data contained, sends to supplier, refuelling is conducted based on information on fuelslip.

For the cargo assignment, the attack methods are –

- Malicious insider with access to cargo assignment document make changes to cargo assignment document before it is sent to service provider.
- Attacker hacks airline mailing list, receives cargo assignment, changes data contained, sends to service provider, loading is conducted based on information on cargo assignment.

RQ2.4: What are the risk impacts?

The risk impacts for the assets identified in passenger management process of the airline turnaround workflow are listed below:

- For the checked-in passenger information, the risk impacts are loss of integrity of luggage information and overloading of the aircraft, loss of integrity of contents of passenger luggage and loss of trust in luggage check-in process.

- For the luggage information, the risk impacts are loss of integrity of luggage information and overloading of the aircraft, loss of integrity of contents of passenger luggage and loss of trust in luggage check-in process.

The risk impacts for the assets identified in ground operations of the airline turnaround workflow are listed below:

- For the fuel-slip, the risk impacts are loss of integrity of fuelslip and lower quantity or different type of fuel can be loaded to the aircraft and data contained in fuelslip can be changed.
- For the cargo assignment, the risk impacts are loss of integrity of cargo assignment document and aircraft is not properly loaded and data contained in cargo assignment can be changed

RQ3: How to mitigate security risks in enterprise collaborations?

In this thesis, the risks identified in the risk analysis section are reduced by applying security requirement and controls for each risk identified. The answer to this research question is provided by answering the specific “what questions” below for each asset identified.

RQ3.1: What are the security requirements?

The security requirements for the reduction of risks identified in the passenger management of airline turnaround workflow are listed as follows:

For the checked-in passenger information, the security requirements are – monitor the activity of check-in personnel and educate the airline passengers on phishing attacks.

For the luggage information, the security requirements are - monitor activities of luggage check-in personnel.

The security requirements for the reduction of risks identified in the ground operations of airline turnaround workflow are listed as follows:

For the fuelslip, the security requirements are – access control on fuelslip document and make the information contained in fuelslip unreadable.

For the cargo assignment, the security requirements are - access control on cargo assignment document and make information contained in cargo assignment unreadable.

RQ3.2: What are the security controls that implement the security requirements?

The security controls for the reduction of risks identified in passenger management of the airline turnaround workflow are listed as follows:

- For the checked-in passenger information, the security controls are – an officer verifies the actions of check-in personnel and using only secured https websites for booking and check-in activity.
- For the luggage information, the security controls are – random checks to verify weight records with actual weight of luggage and installing cameras to record luggage check-in personnel activities.

The security controls for the reduction of risks identified in ground operations of the airline turnaround workflow are listed as follows:

- For the fuelslip, the security controls are – encrypt fuelslip document and verifying all received documents and compare with previous originals received.
- For the cargo assignment, the security controls are – encrypt cargo assignment document and verifying all received documents and compare with previous originals received.

RQ3.3: What degree of security is achieved with implementing the security controls?

The following degree of security is achieved by applying security controls on all the risks identified in airline turnaround workflow –

- Risk1: the risk level was reduced from risk level 12 to risk level 6 and risk reduction level is 6.
- Risk2: the risk level was reduced from risk level 15 to risk level 9 and risk reduction level is 6.

- Risk3: the risk level was reduced from risk level 4 to risk level 2 and risk reduction level is 2.
- Risk4: the risk level was reduced from risk level 15 to risk level 6 and risk reduction level is 9.
- Risk5: the risk level was reduced from risk level 20 to risk level 4 and risk reduction level is 16.
- Risk6: the risk level was reduced from risk level 16 to risk level 4 and risk reduction level is 12.
- Risk7: the risk level was reduced from risk level 12 to risk level 3 and risk reduction level is 9.
- Risk8: the risk level was reduced from risk level 9 to risk level 6 and risk reduction level is 3.

The above research questions and answers to the research questions add up in providing the answer to the main research question of this master thesis - *How to analyse digital security threats in enterprise collaborations?*

Therefore, to analyse digital security threats in enterprise collaborations, the first step is a proper understanding of the workflows involved in the collaborations between the enterprises. This is followed by analyses to identify assets exchanged between collaborating parties in the workflows. The threats and resulting risks on these assets are identified and security controls are applied to mitigate the identified risks. The final step is an evaluation to determine how the applied security controls reduces the identified risks.

7.3 Future works

In the course of this master thesis, some issues have been identified for possible future works. Briefly, we introduce these issues and open up discussions that will provide background for future academic work on these issues.

A Refined method for evaluating risks and prioritizing risk reductions

Organizations have limited resources in combating security risks identified in collaboration with other organizations. It is important for the organizations to identify

which of the poses higher threats in comparison with the other risks identified such that they can focus their limited resources on risks with the highest threats.

In this work, we prioritized risks by comparing graphs involving risk reduction levels, cost of risk reduction and value of business asset. However, this method didn't provide a distinctive result in ranking the risks in the order of greatest importance to the organization. Therefore we suggest that a better approach be developed for evaluating and prioritising risk reductions which will not only provide distinctive risk rankings but also priorities that are relevant to the organizations.

Applying ISSRM Domain models in analysing security threats in cloud supported enterprise collaborations

Initially we set out to analyse security threats in enterprise collaborations including collaborations supported by cloud computing. However the case study analysed in this work didn't present us the opportunity for achieving this. Our worked focused on collaborations where information are exchanged and stored in information systems of the collaborating parties.

Modern organizations are increasingly adopting cloud based technologies and therefore collaborations taking in cloud based environment. Therefore we suggest a further application of ISSRM Domain Models in analysing threats in enterprise collaboration in cloud based environment.

Applying risk based patterns in modelling a secure business process for enterprise collaborations

In this thesis, we analysed threats in enterprise collaborations and also applied security requirements and controls for mitigating these threats. Part of the end result of this work shows how security control applied reduces the risks identified and prioritizes the risks in that order. However this information might not be complete for a security analyst that wishes to redesign the enterprise collaboration workflow in respect to the result of the analyses carried out in this work.

To a provider a better means of presenting the results of analyses carried out in this work, the business processes workflow of the enterprise collaborations have to be remodelled with security aligned business process model notations. Security Risk Oriented patterns [46] is an example of business process models that can be used to redesign a secure workflow for enterprise collaborations.

Therefore, this work can further be extended by using risk patterns in remodelling secure business process workflows for airline turnaround operations discussed in this work.

References

- [1] D. Buhalis eAirlines: *Strategic and tactical use of ICTs in the airline industry* 2003
- [2] Center for Internet Security (CIS), "2013 ANNUAL REPORT," Center for Internet Security, Inc. (CIS), June 19, 2014.
- [3] CNN: *Teen hacker faces federal charges* CNN, 10 March 1997. Available: <http://edition.cnn.com/TECH/computing/9803/18/juvenile.hacker/>. [Accessed]
- [4] The Current State of Cyber Security Readiness in the Aviation Industry Volume 1: *Matter of Time and Money* Author: Sion Camilleri. September, 2014
- [5] A. Costin, A. Francillon Ghost in the Air(Traffic): *On insecurity of ADS-B protocol and practical attacks on ADS-B devices*.
- [6] H. Teso Security Research Team Aircraft Hacking Practical Aero Series April 2013
- [7] A. Costin, A. Francillon Ghost in the Air(Traffic): *On insecurity of ADS-B protocol and practical attacks on ADS-B devices*.
- [8] USA TODAY 27 May 2011: *Air France Jet's final minutes a free-fall* www.usatoday.com/news/world/2011-05-27-air-france-crash_n.htm [Accessed]
- [9] R. Louw, J. Mtsweni: *Guiding principles for adopting and promoting Enterprise 2.0 collaboration technologies*.
- [10] Intralinks, *Sharing Sensitive Corporate Documents Without Compromising Security And Governance* https://www.intralinks.com/sites/default/files/file_attach/white-paper-sharing-sensitive-corporate-documents.pdf [Accessed 31 March, 2016]
- [11] L. Camarinha-Matos: *The Virtual Enterprise Concept* https://www.academia.edu/248717/The_Virtual_Enterprise_Concept
- [12] A. Pinjari, B. R. Mandre. *Cloud-Scheduling Algorithm using Hyper heuristic Approach: Study and Implementation*. June, 2015.
- [13] Honeywell Aerospace: *Onboard Maintenance Systems* <https://aerospace.honeywell.com/products/information-and-maintenancemanagement/onboard-maintenance-systems> (accessed November 2015).
- [14] CSFI: *ATC (Air Traffic Control) Cyber Security Project* <http://www.csfi.us/pubdocs/?id=47> July 16, 2015.
- [15] M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu, R. Krishan, G. Ahn, E Bertino:

Collaboration in Multicloud Computing Environments: Framework and Security Issues.

- [16] A Hevner, S. March, J. Park, S. Ram: Design Science In Information Systems Research. MIS Quaterly Research Essay, March 2004.
- [17] Norta, A. (2012). *Safeguarding Trusted eBusiness Transactions of Lifecycles for CrossEnterprise Collaboration*. Helsinki: University of Helsinki
- [18] N. Ahmed, R. Matulevičius: *Securing business processes using security risk-oriented patterns*. 2013.
- [19] R. Noukkas: Service brokering agreement for an airline, Master thesis, Tallinn University of Technology, 2015.
- [20] ISO/IEC 27005. *Information technology - Security techniques - Information security risk management*. International Organization for Standardization, Geneva, 2008.
- [21] A. Alberts, A. Dorofee: *Managing Information Security Risks: The OCTAVE Approach*, published by Addison Wesley July 09, 2002
- [22] ISO/IEC 27001. *Information technology- Security techniques - Information security management systems - Requirements*. International Organization for Standardization, Geneva, 2005.
- [23] Fontana, J.A., Iyengar, S.S., Pitchford, A.R., Smith, N.R. and Tolbert, D.M., Unisys Corp., 2000. *Software system development framework*. U.S. Patent 6,167,564.
- [24] N. Mayer: *Model-Based Management of Information System Security Risk*, Doctoral Thesis in Computer Science Namur, Belgium, 2009
- [25] A. Alberts, A. Dorofee: *Managing Information Security Risks: The OCTAVE Approach*, published by Addison Wesley July 09, 2002
- [26] Victor R. Basili, Gianluigi Caldiera, Dieter Rombach *THE GOAL QUESTION METRIC APPROACH*
- [27] Security Affairs - *CERT warns that DNS Cache Poisoning attacks could be used also to hijack email to a rogue server and not only to divert the Internet traffic –* <http://securityaffairs.co/wordpress/28283/cyber-crime/dns-cache-poisoning-emails.html> accessed November 2016.
- [28] O. Altuhhova, R. Matulevičius, *An Extension of Business Process Model and Notation for Security Risk Management*, International Journal of Information System Modeling and Design, 4(4), December 2013.

- [29] H. Gluckman *Airline Outsourcing*, Information service group white paper 2013
http://www.isg-one.com/knowledgecenter/whitepapers/private/papers/White_paper_-_Have_Airlines_Outsourced_All_They_Can.pdf, accessed April 2016.
- [30] L. S. Sterling and K. Taveter, *The Art of Agent-Oriented Modeling*, London: The MIT Press, 2009
- [31] J. Ferber, *Multi-agent systems: An introduction to distributed artificial intelligence Addison-Wesley*, Boston, Vol. 222 1999.
- [32] H. Gluckman : *Airline Outsourcing*, Information service group white paper 2013
http://www.isg-ne.com/knowledgecenter/whitepapers/private/papers/White_paper_-_Have_Airlines_Outsourced_All_They_Can.pdf, accessed April 2016
- [33] M. Singhal, S. Chandrasekhar, T. Ge, R. Sandhu, R. Krishan, G. Ahn, E Bertino: Collaboration in Multicloud Computing Environments: Framework and Security Issues. Victor R. Basili, Gianluigi Caldiera, and H. Dieter Rombach. The Goal Question Metric Approach. In *Encyclopedia of Software Engineering*,. John Wiley & Sons, Inc., 1994.
- [34] Gupta, Sunil, and Donald R. Lehmann. "Customers as assets." *Journal of Interactive Marketing* 17.1 (2003)
- [35] US Department of Transportation: *Aircraft weight and balance handbook*
https://www.faa.gov/regulations_policies/handbooks_manuals/aircraft/media/FAA-H-8083-1A.pdf 2007
- [36] NATA Safety *Ist eToolkit*
http://nata.aero/data/files/safety%201st%20documents/etoolkit/safety1st%20etoolkit_24_%20jul-aug%202006.pdf Volume I, Issue 24 – July 18, 2006. Pg 1, accessed April 2015.
- [37] British Standard: *Information technology – Security techniques – Information security management*. BS ISO/IEC 27005: 2008.
- [38] Z. Yazar: A qualitative risk analysis and management tool – CRAMM, Version 1.3, SANS Institute 2002.
- [39] F. Braber, G. Brøndeland, H. Dahl etal: *The CORAS Model-based Method for Security Risk Analysis*. SINTEF, Oslo September 2006.
- [40] A. Alberts, A. Dorofee: *Managing Information Security Risks: The OCTAVE Approach*, published by Addison Wesley July 09, 2002.
- [41] British Standard: *Information technology – Security techniques – Information*

security management. BS ISO/IEC 27005: 2008.

[42] Google postini services *Message Encryption Administration Guide* November 2008

[43] Rein N., *Service brokering environment for airline*, Master Thesis, Tallinn University of Technology, 2014.

[44] Anylogic simulation toolkit: <http://www.anylogic.com/discrete-event-simulation> accessed October 2016.

[45] R. Matulevicius , A. Norta, C. Udokwu, R. Noukas: *Security Risk Management in the Aviation Turnaround Sector* International Conference on Future Data Security Engineering, October 2016.

[46] Ryan K.L. Ko Stephen S.G. Lee Eng Wah Lee, *Business process management (BPM) standards: a survey*, Business Process Management Journal, Vol. 15 Iss 5 (2009).

Appendix 1 – Charts

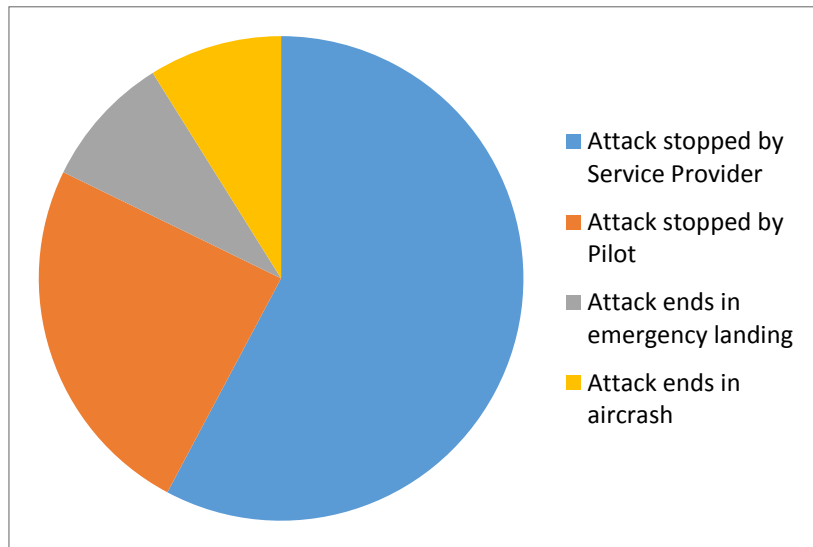


Figure 19. Chart of Airline Refuelling before Application of Security Controls

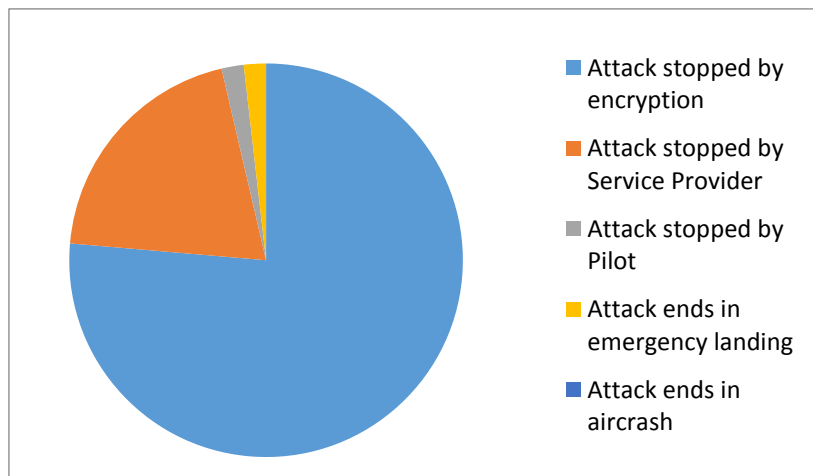


Figure 20. Chart of Airline Refuelling After Application of Security Controls