UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

**Kärt Padur**

# Information Security Risk Assessment in the Context of Outsourcing in a Financial Institution

**Master's Thesis (30 ECTS)**

Supervisor(s): Raimundas Matulevičius, Ph.D
Liis Rebane, Ph.D
Toomas Vaks, MA

Tartu 2019

# Information Security Risk Assessment in the Context of Outsourcing in a Financial Institution

## Abstract:

Information security risk assessment in a financial institution is important for understanding risk exposure to the confidentiality, integrity, and availability of assets. Third-party security is recognized to have a growing importance for financial sector organizations. A financial institution aims for securing information while justifying budgeting decisions. Unfortunately, commonly used methods are dependent on value judgements and individual assurances which limit their reflection of existing uncertainties in reality. This is a problem because organizations do not want to allocate resources into security without accurately estimating their exposure to risks. The paper introduces two information security risk assessment methods: Information System Security Risk Management method and Bayesian Networks Based Attack Graphs. A systematic comparison of the methods is made in the context of third-party outsourcing. A proposition of how to combine a security risk management method together with a probabilistic risk assessment method has been made. Feedback and validation have been given by experts in the field.

## Keywords:

Information security risk assessment, ISSRM, Bayesian Network, Attack graph, Financial institutions, Outsourcing

**CERCS:** T120 Systems engineering, computer technology

## Infoturbe riskijuhtimine finantsettevõttes

### Lühikokkuvõte:

Infoturbe riskihindamine finantsinstitutsioonis on oluline, et mõista ettevõtte varade konfidentsiaalsuse, tervikluse ja käideldavuse riskipositsiooni. Kolmandate osapooltega seotud riskide olulisus on finantsinstitutsioonide jaoks kasvanud. Ettevõtete soov on tagada informatsiooni turvalisus optimeerides samal ajal efektiivselt investeeringuid. Täna on valdavalt kasutusel meetodid, mis tuginevad ekspertide arvamustele ja individuaalsetele hinnangutele, mistõttu kajastavad tulemused vaid limiteeritud vaadet eksisteerivatele riskidele. See on probleem, sest ettevõtted ei soovi teha suure mahulisi investeeringuid turvalisusesse ilma võimalikult täpselt riske hindamata. Käesolevas uurimistöös on käsitletud kahte infoturbe riski hindamise meetodit: ISSRM ja Bayesi võrkudel põhinevat ründepuud. Käsitledes kolmandate osapooltega seotud allhanget kui äriprotsessi, on koostatud süsteemne võrdlus nende meetodite kohta ning hinnatud allhanke korral tekkida võiva riski suurust organisatsioonile. Pakutud on soovitused, kuidas ühendada infoturbe riskijuhtimise metoodika tõenäosusliku riskihindamise metoodikaga. Tulemused on hinnatud valdkonna spetsialistide poolt.

### Võtmesõnad:

Infoturbe riski hindamine, Finantsinstitutsioonid, ISSRM, Bayesi võrgud, Ründepuu
**CERCS:** T120 Süsteemitehnoloogia, arvutitehnoloogia

## Table of Contents

## List of Figures

# List of Tables

## Terms and Notations

| Term | Description |
|---|---|
| BN | Bayesian Network |
| BNBAG | Bayesian Network Based Attack Graph |
| BPMN | Business Process Modelling Notation |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission |
| CWE | Common Weakness Enumeration |
| DAG | Directed Acyclic Graph |
| DDoS | Distributed Denial of Service |
| EBA | European Banking Authority |
| ENISA | European Union Agency for Network and Information Security |
| FAIR | Factor Analysis of Information Risk |
| FSA | Financial Stability Authority |
| IEC | International Electrotechnical Commission |
| IRAM | Information Risk Assessment Methodology |
| IS | Information System |
| ISO | International Organization for Standardization |
| ISSRM | Information System Security Risk Management |
| MiFID | Markets in Financial Instruments Directive |
| NIST | National Institute of Standards and Technology |
| NPT | Node Probability Table |
| OCTAVE | Operationally Critical Threat, Asset, and Vulnerability Evaluation |
| OWASP | Open Web Application Security Project |
| PSD2 | Payment Services Directive 2 |

# 1 Introduction

The past few decades have been leading the way of extensive use of and dependence on information communication technology and exponential growth of new data. According to the International Telecommunication Union [1] [2], the total amount of Internet users has increased from 23% to 51% of the whole population during the last ten years. International Data Corporation (IDC) [3] estimates that by 2025 the global amount of data will grow about ten times bigger compared with the amount of data that was generated in 2018. While a significant increase in the use of technology and information has introduced new opportunities, such changes in society bring non-traditional risks to organizations and individuals [4]. In the 1950s, it was suggested that it is not enough for an organization to do investment decisions purely using the average return of investment, but risks should also be considered [5]. Although this revolutionary way of thinking was first established in the portfolio investment field, now this principle is also generalized to other areas.

The research work illustrates how information security risk assessment methods can be applied in the outsourcing system of a financial institution. Risk assessment is part of risk management. The process consists of risk identification, analysis, and evaluation according to the ISO 31000:2018 standard [6]. Information security risk assessment should be conducted to "*identify risks associated with the loss of confidentiality, integrity, and availability for information within the scope of the information security management system*" [7]. Two methods – Information System Security Risk Management (ISSRM) [8] and Bayesian Network Based Attack Graph (BNBAG) [9] [10] – are used to assess the information security risk. ISSRM represents a security risk management method and BNBAG has the characteristics of a probabilistic risk assessment method. Both methods are used to assess the information security risk of outsourcing system. Outsourcing is defined as "*the regulated entity's use of a third party* [– – –] *to perform activities on a continuing basis that would normally be undertaken by the regulated entity, now or in the future*" [11]. The assets of outsourcing are defined, threats, vulnerabilities, and impact analysed, and risk assessed. A financial institution has contributed to the research to assess their information security risk of outsourcing system.

Industry sector organizations, including financial institutions, want to pursue their business ambitions while operating in a secure environment. Hence, the information security risk to the organization has to be assessed. In addition to securing their own information systems, where financial institutions have already made significant investments, risk arising from third-party security is recognized to have a growing importance for financial sector organizations [12]. The volume of outsourcing is growing which gives an opportunity for the threat to target vulnerabilities in shared banking systems and third-party networks [12]. Today, financial institutions use qualitative security risk management methods which take value judgements as input to the analysis [13]. It saves time, effort, and expenses [14]. However, most of the methods rely on subjective judgment, focus on concepts and principles, and do not provide monetary values [9]. Alternatively, the use of quantitative probabilistic risk assessment methods, which use measured data as input to limit subjectivity of the analysis, can be considered. However, the process of gathering data and managing it requires more time and effort [13]. The third possibility is to combine the two together into a hybrid method, which allows the use of subjective and measured data as input while optimizing time, effort and expenses [14].

As security risk management methods and probabilistic risk assessment methods have limitations to consider, enhancements to the information security risk assessment methods are required. The developed method should combine the benefits of both methods while reducing their limitations. It should include the identification of assets that need protection, coherent analysis of threats, incorporation of dependencies between information system vulnerabilities, and defined impact. The aim of comprehensive and accurate risk assessment is the optimal allocation of limited resources for efficient risk reduction. The following question is the main research question proposed as the purpose of this research paper. It is developed further into the four research questions.

**How to combine security risk management and probabilistic risk assessment methods?**

*Research question 1: What are the assets that need protection?* Asset identification is the primary task when assessing information security risk. An answer to this question defines the context of the study and identifies the relevant assets that need protection. ISSRM [8] method is used to scope the assets.

*Research question 2: What is the estimated information security risk?* An answer to this question shows the information security risk assessment process. Risk is assessed using the defined assets in Research question 1. ISSRM method [8] is chosen as an example of security risk management method and BNBAG [9] [10] approach as an example of a probabilistic risk assessment method.

*Research question 3: What is the comparison of the chosen risk assessment methods?* An answer to this question shows the difference between assessing risk using security risk management method or probabilistic risk assessment method. The assessment results from Research question 2 have been compared.

*Research question 4: How can security risk management method and probabilistic risk assessment method be used together?* An answer proposes a list of steps to combine a security risk management method with a probabilistic risk assessment method to address the challenging parts of risk assessment processes.

Questions 1 – 3 are answered using an outsourcing scenario proposed by the financial institution. Research questions 1 – 4 provide understanding about combining security risk assessment methodology with probabilistic risk assessment method for improved results, highlighting potential benefits, limitations and necessary prerequisites.

The academic literature presents a coherent overview of information security risk assessment methods. Despite that, relevant contribution to the existing literature has been made. Firstly, assets that need protection in an outsourcing system have been identified. Secondly, two applicable methods, both different in nature, have been used to assess the risk of outsourcing system for the financial institution.  Thirdly, a comparison of the assessment methods has been represented. A proposition of how to combine a security risk management method together with a probabilistic risk assessment method has been made. Feedback and validation of the research work have been given by the experts from the financial institution.

The structure of the research paper is represented as follows: Chapter 1 is the introduction of the scope, research problem, research questions, and contribution of the author; Chapter 2 is the theoretical overview of information security risk assessment methods; Chapter 3 is the case study description of outsourcing system in the financial institution; Chapter 4 is the information risk assessment using ISSRM method; Chapter 5 is the information risk assessment using BNBAG method; Chapter 6 is a discussion of the results; and Chapter 7 is the conclusion of the research paper.

# 2 Theoretical Framework

This chapter focuses on the state of the art of information security risk assessment. An overview of the existing risk management standards is introduced. Two methods – ISSRM and BNBAG – are described in detail as they are the focus of this research paper. The processes of gathering data, methods for calculating the result and the meaning of the results of these methods are explained. A comparison of these methods is included to map the similarities and differences between the two methods.

## 2.1 Information Security Risk Management Standards and Frameworks

There is a number of information security risk management standards and frameworks available for organizations to use. Firstly, ISO/IEC 27005 [15], which is one of the ISO/IEC 2700x standards [16], is an information security risk management standard. Risk assessment consists of risk identification, analysis, and evaluation [7].

Secondly, NIST has developed their information risk management standard named NIST 800-30 "Risk Management Guide for Information Technology Systems" [17]. It is known for its flexibility; therefore, it has been adopted by a number of organizations.

There are other risk assessment standards and frameworks available, e.g. FAIR approach [18], OCTAVE Allegro framework [19], COSO framework [20]. Regardless, ISO/IEC 27005 and NIST 800-30 are the most famous ones.

The research focuses on information security risk assessment in a financial institution. After having reviewed the relevant literature, there is no specific information security risk management standard or framework for financial institutions. Financial Sector Advisory Centre of World Bank [21] has issued a document listing a number of relevant financial sector specific documents that stress the issues of security risk assessment and offer guidelines.

**Classification of Information Security Risk Assessment Methods**

An information security risk assessment method should have the characteristics that describe each one of the following four classes [14]:

1. Qualitative, quantitative, or hybrid – different in their input and output requirements.
2. Asset-driven, service-driven, or business-driven – a different level of organization is being focused on.
3. Horizontal or vertical – different in their resource valuation.
4. Non-propagated or propagated – different in their attack propagation approach.

ISSRM and BNBAG methods have been mapped using the categorization to make them comparable with other methods. The results are shown in Table 4.

## 2.2 Information Systems Security Risk Management Method

ISSRM method [8] is an information security risk management method. It helps to understand which assets are valuable and need protection against certain threats. Also, it introduces risk treatment options by proposed security countermeasures. It offers a domain model, metrics and process for managing risk. The first reason why ISSRM has been chosen is due to its qualitative nature which is different from the other method. The second reason is due to its similarity to Information Risk Assessment Methodology 2 (IRAM 2). Initially, IRAM 2 was considered to be analysed because it has been used in the financial institution before. Unfortunately, the author of the thesis was not able to get permission from the Information Security Forum to use their method. ISSRM has similar characteristics and elements compared with IRAM 2, therefore, it is a suitable alternative to use.

### 2.2.1 Domain Model

The ISSRM domain model [8] has been developed through a survey of security risk management standards and methods. The domain model for ISSRM, presented in Figure 1., has three groups of concepts: asset-related concepts, risk-related concepts, and risk-treatment related concepts which are marked accordingly with yellow, red and green. The current section and the following two sections are based on the research by Dubois *et al.* [8].

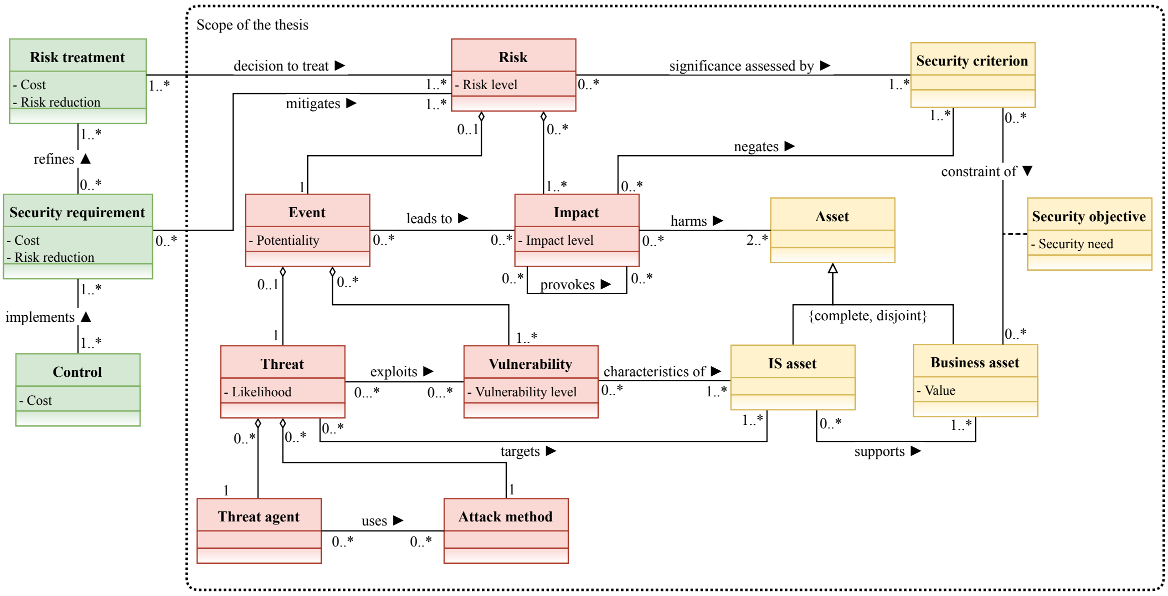


Figure 1. ISSRM domain model (adapted from [11])

*Asset-related concepts* emphasize which assets are important to be protected according to the security needs of the system. *Assets* are either *business assets* or *information system (IS) assets*. A business asset is any information, process or skill that is necessary for an organization to achieve its business objectives. It is characterized by the *security criterion* of confidentiality, availability, or integrity. Information system assets are valuable parts of IS because they provide support for business assets.

The second group is *risk-related concepts* which illustrate risk and its components. *Risk* is described as a *threat* that could exploit one or more *vulnerabilities*, leading to an *impact* that harms two or more assets and negates the security criterion. A threat is a combination of a *threat agent* and *attack method*.

*Risk treatment-related concepts* describe how to treat risk based on the knowledge of existing *controls* that implement *security requirements* which mitigate *risk*. Risk treatment is the decision whether to avoid, reduce, transfer or retain the risk. Risk treatment-related concepts are not part of the scope of the thesis.

### 2.2.2 Metrics

ISSRM method [8] offers several metrics. Firstly, the *value* metric describes the value of a business asset considering the potential impact if the business asset is either disclosed, modified or disrupted. Secondly, the *security need* metric expresses the importance of the security criterion with respect to the business asset. These two metrics describe asset-related concepts.

Thirdly, the *likelihood* metric describes the likelihood of an attack considering the adversary’s motivation and attack method sophistication. *Vulnerability level* metric describes the prevalence of the vulnerability and the likelihood of exploit. *Potentiality* is calculated using the likelihood and vulnerability level metrics represented in Equation 1. *Impact level* metric is the maximum value that is assigned to the security need metric.

$$\mathit{Potentiality} = \mathit{Likelihood} + \mathit{Vulnerability} - 1 \qquad (1)$$

*Risk level* metric is calculated as the product of *potentiality* and *impact level*. It is calculated according to Equation 2. These five metrics describe risk-related concepts.

$$\mathit{Risk\ level} = \mathit{Potentiality} \times \mathit{Impact} \qquad (2)$$

In risk treatment-related concepts, risk treatment and security requirements are estimated using *risk reduction* and *cost*. Controls are estimated in terms of *cost*. These metrics are not used in the case study part of the thesis.

### 2.2.3 ISSRM Process

The process of ISSRM [8] introduces the activities to conduct information security risk management. The overall process is presented in Figure 4. It begins with understanding the *context* where the organization is operating and *identifying* its *business* and *IS assets*. The next step is to determine the *security objectives* in terms of confidentiality, integrity, and availability based on the level of protection needed for the assets. Then the *risk* is *analyzed* and *assessed*. After these activities, it is decided whether the assessment is satisfying or not. These previous steps can be iterated in case of unsatisfying results.

The following step is about *risk treatment* whether to avoid, reduce, transfer, or accept the risk. Then *security requirements* are to be defined to state the needed security conditions to achieve the desired level of security based on identified risks. If the treatment has been unsatisfying, then the whole process can be started from the beginning or from risk treatment step. The last step is about *selecting* and *implementing controls* based on security requirements.

The first three steps form risk assessment; thus, they are considered in the case study of the thesis. Risk treatment, security requirement definitions, and controls are left out of the research.

**Modelling threats and vulnerabilities**

Part of ISSRM process is risk analysis and assessment. ISSRM method considers the risk to be the successful exploit of a *vulnerability* by a *threat* leading to an impact which harms an asset and negates the security criterion according to the domain model. Therefore, threats and vulnerabilities have been modelled.

Threats can be modelled following a taxonomy, e.g. MITRE's ATT&CK taxonomy [22]; Threat Agent Library by Intel Corporation [23], or some other. The chosen taxonomy

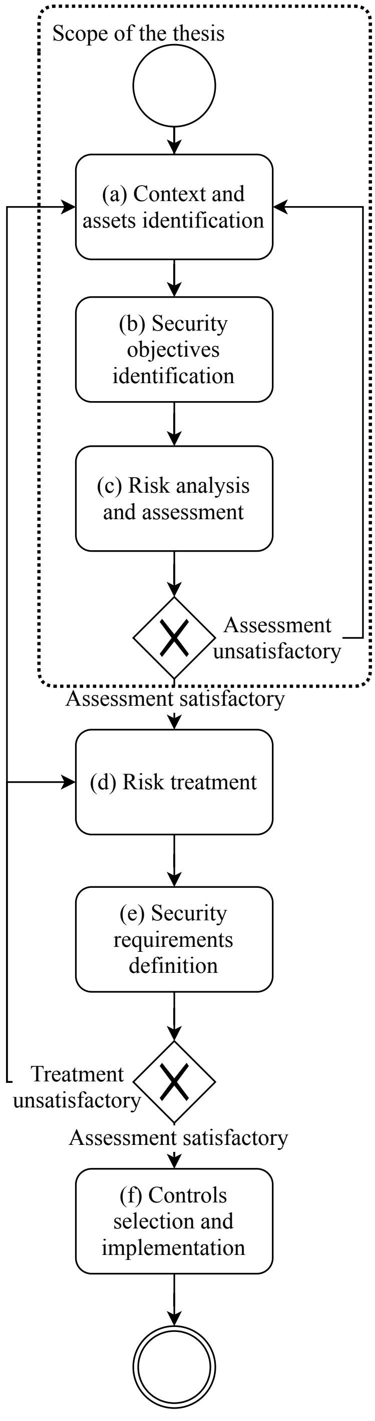

Scope of the thesis
(a) Context and assets identification
(b) Security objectives identification
(c) Risk analysis and assessment
Assessment unsatisfactory
Assessment satisfactory
(d) Risk treatment
(e) Security requirements definition
Treatment unsatisfactory
Assessment satisfactory
(f) Controls selection and implementation

Figure 2. ISSRM process (adapted from [11])

is issued by the European Union Agency for Network and Information Security (ENISA) [24] as it categorizes threats similar to the categorization in IRAM 2. As noted, the author was not able to get permission from ISF to use IRAM 2 which has been used in the financial institution before. ENISA taxonomy categorizes threats into the following classes [24]:

1. Unintentional damage, which refers to the loss of confidentiality, integrity or availability of assets due to mistakes or errors.
2. A disaster which occurs due to natural or environmental forces.
3. Failures or malfunction which occurs without somebody causing them.
4. Outages which occur due to unavailability of resources without them being attacked.
5. Intentional physical attack, which refers to the physical damage on assets by humans.
6. Nefarious activity which indicates any malicious or abusive activity towards information systems.
7. Interception which is a deliberate attack against the information system to alter communication.

Secondly, there are lists of vulnerabilities available, e.g. MITRE Common Vulnerabilities and Exposures [25], or NIST National Vulnerability Database repository [26]. The chosen taxonomy to model vulnerabilities is OWASP Top 10 (2017) as it has been used by the financial institution before. An overview of the OWASP Top 10 categories is presented in the following list [27]:

1. Injection – a threat agent can send malicious code to the interpreter.
2. Broken authentication – a system has authentication weaknesses in it.
3. Sensitive data exposure – data is not protected according to the needs.
4. XML external entities – an application parses xml input.
5. Broken access control – user of the system can act according to different permissions than one is intended to.
6. Security misconfiguration – threat agent can gain access to the system due to the lack of proper configuration.
7. Cross-Site Scripting – malicious code can be executed by a threat agent in another user’s browser.
8. Insecure deserialization – untrusted user input is used while rebuilding data format to an object.
9. Using components with known vulnerabilities – known vulnerabilities are not patched.
10. Insufficient logging and monitoring – a threat agent can achieve the goal without even being detected due to lack of logging and monitoring of systems.

Certain vulnerabilities have been chosen from the categories and adjusted according to the nature of the case study. An overview of the vulnerabilities is provided in Appendix I.

## 2.3 Bayesian Networks Based Attack Graphs Method

BNBAG method [9] [10] is a probabilistic risk assessment method. Bayesian Network (BN) is used to model and analyse an attack graph. The reason why BNBAG is used as an approach to model information security risk is its difference from ISSRM model. The financial institution about which the research is conducted has expressed their interest in potentially evaluating some parts of information security risks quantitatively. As the financial institution is not able to provide complete data for the analysis, a hybrid method as BNBAG is a suitable one.

### 2.3.1 Bayesian Probability Theory

Bayes' probability theorem provides a version to compute conditional probabilities. Bayesian probabilistic reasoning starts with a hypothesis, $H$, for which the probability of hypothesis *P(H)* is called prior belief about *H*. Evidence, *E*, is used to revise the belief about *H* using the likelihood of evidence, *P(H|E).* The posterior belief about *H* in the light of evidence is calculated [9]. Bayes' theorem states that the probability of the hypothesis given the evidence is equal to the probability of the evidence given the hypothesis times the probability of hypothesis divided by the probability of evidence [28]. Bayes' theorem is represented in the following Equation 3. [28]:

$$P(H|E) = \frac{P(E|H) \times P(H)}{P(E)} \tag{3}$$

where

| | |
|---|---|
| *P(H)* – | prior belief about H, |
| *P(E)* – | probability of evidence, |
| *P(E\|H)* – | likelihood of evidence E, |
| *P(H\|E)* – | posterior belief about H. |

There are situations where there is no information about *P(E),* then marginalization, i.e. the sum of probabilities of all events, can be used following Equation 4. [9]:

$$P(E) = \sum_h P(E, H) \tag{4}$$

where

| | |
|---|---|
| *P(E)* – | probability of evidence, |
| *P(E,H)* – | probability of evidence and probability of hypothesis. |

Bayes' theorem allows to renew and change the estimates if new data has been gathered. If there is a strong prior belief that some hypothesis is true, then after having gained more data that fails to support the hypothesis, Bayes' theorem will favour the alternative hypothesis that better explains the data [9].

### 2.3.2 Attack Graphs

An attack graph with a structure of a tree provides a useful framework to represent information system vulnerabilities and dependencies between them. An attack graph shows the possible attack vectors to compromise a given objective by successfully exploiting vulnerabilities in sequence [10]. All the vulnerabilities that form the attack vector must be successfully exploited. There can be several attack paths through the system to reach the main goal.

Logical attack graphs rely on the monotonicity principle, i.e. once an attacker has gained privileges, one will not give them away [10]. Monotonicity introduces DAGs, i.e. there is a directed non-circular movement between the structure of nodes [9]. A simple example of a DAG graph is presented in Figure 3. The arcs from A to B, from B to D, and from C to D mean that there is a directed causal dependence of A on B, and of B on D, and of C on D. There cannot be an arc from D to A due to the acyclic structure of the graph.

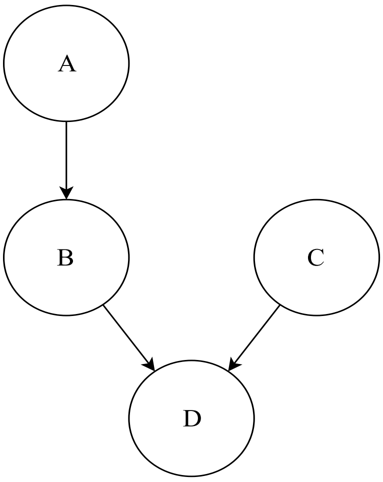


Figure 3. DAG structure example

The occurrence of an event in the attack tree is modelled probabilistically. These models contain one or many parameters, which values are known only with uncertainty [29]. An attack graph is categorized as a qualitative model as it considers an information system to be either secure or not [30].

### 2.3.3 BNBAG Process

BN is the set of variables represented as nodes and the direct dependences between the edges of these nodes. It is in the form of a DAG and has a set of node probability tables (NPTs) [9]. The process of assessing information security risks with BNBAG is represented in Figure 4. It consists of the following steps: (1) identification of the possible set of vulnerabilities  in the system; (2) creation of the vulnerability nodes, i.e. and directed arcs between the nodes where an occurrence of an exploit is conditioned on the exploit of the previous one; (3) specification of the NPT for each vulnerability node; (4) reasoning and calculation.

The steps of (1) identification of vulnerabilities and (2) the creation of directed arcs between them have been done following the OWASP Top 10 taxonomy introduced in the ISSRM process description in Section 2.2.3. Overview of the vulnerabilities is presented in Appendix I.

The third step is about NPTs. The NPT is a table of probabilities that represent the probability distribution of the node given its parents [9]. NPTs incorporate the conditional probability distribution which is the information about each node in the BNBAG.  is a node, represents the parent node(s), and is the probability of a node becoming successful given the state of its parent node(s)  [10]. According to Figure 3., a NPT of D is the probability distribution of D given the set of parents of D which are B and C; a NPT of B is the probability distribution of B given its parent A. If a node does not have parents, the NPT is simply the probability distribution of that node. In Figure 3., node A and node C do not have any parents therefore the NPT of A is the probability distribution of A and the NPT of C is the probability distribution of C. Any pair of variables that are not connected to each other indicate independence between them.

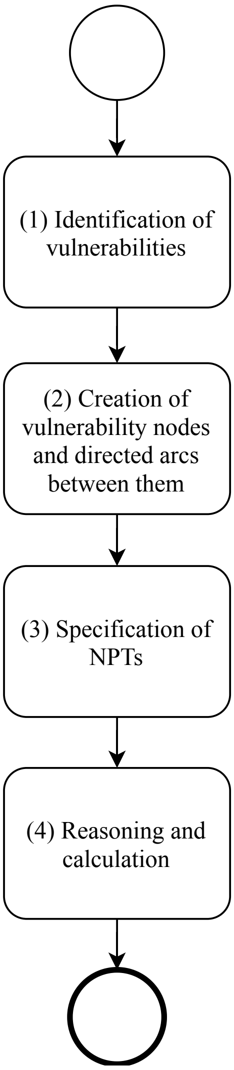

(1) Identification of vulnerabilities
(2) Creation of vulnerability nodes and directed arcs between them
(3) Specification of NPTs
(4) Reasoning and calculation

Figure 4. BNBAG process

The fourth step is about calculating the result. In risk assessment, an incident can happen only if one or more vulnerabilities are exploited.

Equation 5. indicates that if an incident is true given that the vulnerability is true, then it equals to the probability of the vulnerability. Equation 6. indicates that if there are no vulnerabilities in the system, then there is no incident. Equation 7. indicates that if there is an exploit of the vulnerability, then there could potentially be no incident. Equation 8. indicates that if there are no vulnerabilities, then there are no incidents. To calculate the NPT for an incident, the following Equations 6 to 9 are used inside the NPT cells:

$$P(Incident=T|Vulnerability=T)=P(Vulnerability) \tag{5}$$

$$P(Incident=T|Vulnerability=F)=0 \tag{6}$$

$$P(Incident=F|Vulnerability=T)=1\text{-}P(Vulnerability) \tag{7}$$

$$P(Incident=F|Vulnerability=F)=1 \tag{8}$$

Therefore, the probability of an incident in the system is the probability that at least one of the vulnerabilities becomes exploited. Equation 9. describes the probability of an incident:

$$P(Incident=T)=1 - \prod P(vulnerabilities=F) \tag{9}$$

A BN can be constructed qualitatively, automatically from data, or using a combination of them both. The construction of attack graphs and calculations can be labour-intensive as it requires a lot of skill, expertise, and creativity. Also, the communication between the experts needs to be intense and productive [31]. It is positive that once the construction is ready, the BN parameters can be continuously updated as new information arrives.

## 2.4 Comparison of ISSRM and BNBAG

ISSRM and BNBAG methods have similarities and differences in their process of assessing risk, concepts that are being used, the purpose and variables. Three tables are made to describe this information and give an overview. Table 1. is made to compare the methods in the context of their process, according to Figure 2. and Figure 4.

Table 1. Comparison of the processes of ISSRM and BNBAG

| Process overview | ISSRM | BNBAG |
|---|---|---|
| Defining the risk assessment scope | (a) Identifying business and IS assets<br>(b) Determining security objectives | (1) Identifying the vulnerabilities |
| Defining the relevant threats and potential vulnerabilities, calculating the risk | (c) Risk analysis and assessment | (2) Creating the vulnerability nodes and the directed arcs between the nodes<br>(3) Specifying the NPTs<br>(4) Reasoning and calculation |
| Deciding on the risk treatment | (d) Risk treatment<br>(e) Security requirements definition | - |
| Implementing relevant controls | (f) Controls selection and implementation | - |

Source: Compiled by the author (based on the Figure 2. and Figure 4.)
Notes: 1) the symbol "-" indicates that this part of the process is not included in the method.
2) (d), (e), (f) parts of the process are not analysed in the empirical part of the study.

Firstly, the process of *identifying business and IS assets* and *determining the security objectives* in ISSRM are done to scope the relevant assets. BNBAG do not scope assets, instead, the relevant vulnerabilities are determined which is described by *identifying the vulnerabilities*. Secondly, *risk analysis and assessment* are done to determine the relevant threat agents and their attack methods that are used to exploit one or many vulnerabilities which leads to an impact for the company. The reason for this phase is to calculate the risk level according to ISSRM. In BNBAG, the second phase is done by *creating the vulnerability nodes*, *creating arcs between conditioned attack nodes*, *specifying the NPSs*, and *calculating the probability of an incident*. The reason for this phase is to analyse the vulnerabilities to calculate the probability of a vulnerability becoming exploited. Although the two methods are fairly different in their nature, this mapping is used in the thesis for further analysis. ISSRM is a risk management method, therefore, risk treatment and controls selection are considered as part of the process. *Risk treatment* and *defining security requirements* steps are taken to decide on the risk treatment plans. Also, ISSRM deals with *controls selection and implementation* to decide on the relevant controls to implement the security requirements that mitigate the risk. As BNBAG is a probabilistic risk assessment method, it does not consider risk treatment, security requirements nor controls as part of its process.

Table 2. represents the comparison between the ISSRM domain model and BNBAG method.

Table 2. Comparison of the models of ISSRM and BNBAG

| **Model overview** | **ISSRM** | **BNBAG** |
|---|---|---|
| Finding the relevant assets and determining their need of security in terms of confidentiality, integrity, and availability | IS asset<br>Business asset<br>Asset<br>Security objective<br>Security criterion | - |
| Defining the possible threats agents, their attack methods and the probability of a successful attack | Threat agent<br>Attack method<br>Threat | Node probability table |
| Identifying the vulnerabilities and their dependence on each other | Vulnerability | Vulnerabilities<br>Dependencies between vulnerabilities |
| Defining the probability of a successful attack | Event | Probability of incident |
| Identifying the impact of a possible attack | Impact | - |
| Finding the amount of risk | Risk | - |
| Deciding on the risk treatment options | Risk treatment<br>Control | - |
| Defining the needed security | Security requirement | - |

Source: Compiled by the author (based on Sections 2.2 and 2.3.)

Notes: 1) the symbol "-" indicates that this part of the process is not included in the method;
2) parts of the model – risk treatment, control, and security requirement – are not analysed in the case study.

The first part of the domain model of ISSRM consists of *IS assets*, *business assets*, which together form *assets*. Also, *security objective* and *security criterion* in terms of confidentiality, integrity, and availability are studied. The reason is to describe the relevant IS and business assets in terms of their need for confidentiality (C), integrity (I) and availability (A). BNBAG does not include assets and their need for security in terms of C-I-A to be analysed.

A *threat* in ISSRM is defined as an individual or a group of people with certain attributes, e.g. motivation and capability, and their *attack method* which indicates their actions taken to target the IS assets. These two domains are put together which results as a *threat.* BNBAG describes a threat using *node probability tables* that describe the probability of a vulnerability being exploited by an attacker assuming its existence in the system. BNBAG does not consider a threat with exact attributes. A *vulnerability* in ISSRM is a weakness of IS asset which can be exploited by a threat. In BNBAG, the focus is on determining the *vulnerabilities* of the system or process and various *dependencies between* defined *vulnerabilities*. An *event*, in ISSRM, is successful exploitation of a vulnerability by a threat. BNBAG describes a similar situation with the *probability of an incident*, which is the probability of successful exploitation of the vulnerability.

BNBAG does not have any other parts in its model to assess information security risk. ISSRM domain model is much richer in that sense having a number of components incorporated into risk assessment. The *impact* is the potential result in terms of loss after a successful attack. *Risk* is as an event and its corresponding impact. When the risk is found, it is decided how to *treat* it based on the knowledge of existing *controls* that implement *security requirements*.

ISSRM and BNBAG use variables in the process of risk assessment. The comparison of variables is presented in Table 3. ISSRM uses the metric of *value* and *security need* to determine the value of a business asset in terms of confidentiality, integrity, and availability. BNBAG does not consider asset related metrics. ISSRM uses *likelihood* to determine the probability of a threat. BNBAG does not explicitly use any variables to describe a threat. ISSRM uses *vulnerability level* metric to determine the level of weakness. BNBAG also uses *vulnerabilities* to describe the probability of discovering certain weaknesses in the system that could become exploited. ISSRM calculates the *potentiality* to describe the likelihood of a threat event happening. BNBAG uses *probability* to estimate the probability of a vulnerability becoming exploited by a threat. ISSRM uses *impact level* to determine the impact of a successful threat event. BNBAG does not consider impact calculation as part of the risk assessment process. The main goal of ISSRM is to calculate the *risk level* that describes the risk. The aim of BNBAG is to calculate the *probability of incident* that describes a probability of an attack against one or many vulnerabilities found in the information system that result as a risk to an organization. ISSRM also uses *cost* and *risk reduction* metrics to describe risk treatment, security requirements, and controls. BNBAG does not consider risk treatment and controls as part of it.

The two methods can be compared in terms of the classification of qualitative, quantitative and hybrid approaches and to the taxonomy introduced by Shameli-Sendi *et al.* [14]. The Table 4. has been presented to give a short overview of the classification of ISSRM and BNBAG methods introduced in Section 2.1. The distinguishable characteristics that describe these methods are also presented in Table 4.

Table 3. Comparison of the variables of ISSRM and BNBAG

| **Description of the variables** | **ISSRM** | **BNBAG** |
|---|---|---|
| The value of business and IS assets | Value | - |
| The security need of assets | Security need | - |
| The possible treats, their likelihood of initiating a successful attack and their strength | Likelihood | - |
| The vulnerabilities of the system | Vulnerability level | Vulnerabilities |
| The probability of a successful attack against the system | Potentiality | Probability |
| The impact of a successful attack | Impact level | - |
| The amount of risk | Risk level | Probability of incident |
| The cost of risk treatment and the amount of risk reduction | Cost of risk treatment<br>Risk reduction due to risk treatment | - |
| The cost of security requirements and the amount of risk reduction | Cost of security requirement<br>Risk reduction due to security requirement | - |
| The cost of controls | Cost of control | - |

Source: Compiled by the author (based on Sections 2.2 and 2.3)

Notes: 1) the symbol "-" indicates that this part of the process is not included in the method.
2) the metrics – cost of risk treatment, risk reduction due to risk treatment, cost of security requirement, risk reduction due to security requirement, cost of control – are not analysed in the case study.

The following paragraphs illustrate how ISSRM and BNBAG fit in the taxonomy proposed by Shameli-Sendi *et al.* [14]. Information security risk assessment *appraisements* are traditionally classified as qualitative, quantitative, or hybrid [14]. ISSRM method is a qualitative method because it uses subjective judgement values or range variables as input to the analysis and results in a rank of risks. BNBAG is a hybrid method because it uses either numeric or subjective judgement values as input to the analysis and outputs the probability of an incident calculated using Bayesian statistics.

Information security risk assessment can be done in three *perspectives* classified as asset-driven, service-driven, or business-driven [14]. Although, these three are the most common ones, the author of this research has also proposed a vulnerability-driven perspective. ISSRM has the asset-related concept, risk-related concept and risk-treatment-related concept incorporated into the method. Despite that, the main focus in on securing the assets in terms of confidentiality, integrity, and availability. BNBAG is a vulnerability-driven perspective as the main focus in on identifying the vulnerabilities and the potential incident when one or more vulnerabilities have been exploited.

Table 4. Characteristics of ISSRM and BNBAG

| **Characteristics** | **ISSRM** | **BNBAG** |
|---|---|---|
| Appraisement | Qualitative | Hybrid |
| Input/output | Range/rank | Non-monetary/non-monetary |
| Perspective | Asset-driven | Vulnerability-driven |
| Resource Valuation | V(I)+H(I) | H(D) |
| Risk Measurement | Non-propagated | Propagated |
| Calculation technique | Multiplication operation | Bayesian network-based attack graph |
| Assessment stages | (1) RA; (2) RE; (3) RR | (1) RA; (2) RE |
| Result | Risk level | Probability of incident |

Source: Compiled by the author (based on the classification by Shameli-Sendi *et al.* [14])

Resource valuation is the phase of risk analysis that defines the value of resources [14]. The *vertical resource valuation* considers the degree of contribution of a resource to upper levels. ISSRM evaluates assets to be independent *(V(I))* without contributing to other levels. Also, the resources are evaluated independently *(H(I))*. BNBAG does not consider assets as part of the analysis but evaluates resources dependently *(H(D))*.

The last step of risk assessment is risk measurement where two types of measurements are distinguishable: non-propagated or propagated [14]. ISSRM considers impact only in terms of loss in confidentiality, integrity or availability of one asset which is the reason why it is a non-propagated type of a method. BNBAG is a propagated type as it uses conditional probabilities. It measures a probability of a vulnerability being exploited conditioned on its parents being successfully exploited.

The other characteristics to describe the methods are *calculation technique*, *assessment stages*, and *result*. ISSRM uses *multiplication operation* to calculate the risk as the product of impact and likelihood. BNBAG uses *Bayesian network-based attack graph* to calculate the probability of a successful incident. In BNBAG, the risk is a state of uncertainty calculated by using Bayesian probability theory and the characteristics of an attack graph. Risk assessment stages – *risk analysis* (*RA*), *risk evaluation* (*RE*) and *responding to risk* (*RR*) – have been described in detail in previous sections. ISSRM method incorporates all the stages, while BNBAG does not consider RR. All in all, the result of methods that are relevant to this research are *risk level* and the *probability of an incident*.

## 2.5 Chapter Summary

This chapter introduced the state of the art of information security risk assessment standards, frameworks and methods. Firstly, an overview of the information security risk management standards and frameworks has been provided. Secondly, a possible classification taxonomy of information security risk assessment methods has been presented. The main focus of this chapter has been on giving an overview of the ISSRM and BNBAG methods in the context of their processes, domain models and metrics. Information about the data gathering processes, result calculation methods, and the meaning of the results has been provided.

The comparison of ISSRM and BNBAG has been done as a mapping between the relevant stages, domain models and metrics of these methods. Also, ISSRM, and BNBAG has been compared in the context of the classification taxonomy, which helps to compare them also with other methods that are out of the scope of this thesis. The chapter has given an overview of the available standards, frameworks and methods that can be used in information security risk assessment in an organization.

# 3 Case Description

The chapter introduces the case study in the context of a financial institution. The focus is on evaluating information security risk that could potentially characterize outsourcing. The outsourcing system and its components have been introduced. Also, outsourcing as a business process has been modelled and visualized to give an overview of its complexity.

## 3.1 Outsourcing in Financial Institutions

Today it is common for organizations to outsource certain products or services to third-party organizations. The reasons to outsource can be different, e.g. getting access to better skills, expertise, and technology, inability to provide services internally, wanting to concentrate on core business processes, optimizing the use of in-house personnel, reducing cost and improving flexibility [32]. The main problem associated with outsourcing is limited control over the services and solutions developed or maintained by a third-party entity [33]. Due to the dependence between the outsourcing organization and the third-party entity, the risks that the third-party is facing can also have an impact on the outsourcing organization [33].

Financial institutions are highly regulated organizations. In Estonia, according to the Emergency Act chapter 5 [34], payment service providers have been listed as vital service providers which "*is a service that has an overwhelming impact on the functioning of society and the interruption of which is an immediate threat to the life or health of people or to the operation of another vital service or service of general interest*" [34]. Financial institutions need to comply with rules and regulations. Third-parties are usually unregulated and they might not understand the importance of the regulations [35]. According to the Basel Committee on Banking Supervision [11], the financial service provider that wants to outsource a number of services and solutions is responsible for managing and monitoring the unregulated party's activities. The topic of outsourcing in covered in a number of regulations that the financial institutions need to follow, e.g. Directive 2014/65/EU known as the Markets in Financial Instruments Directive (MiFID) [36], and the Directive 2015/2366/EU known as the Payment Services Directive 2 (PSD2) [37].

The services provided by third-party vendors can be classified into the following categories: telecommunication, security, data management, software, hardware, automation, and information systems services. Telecommunication service vendors are providing WAN networking solutions, SWIFT common components, web site hosting, VoIP, Internet access, and data lines. A security service that has been outsourced is a solution to protect the organization from DDoS attacks. Some of the data centre related solutions that belong to data management services have also been outsourced. Software development that has been outsourced is mainly associated with mobile application development and integration. Also, some software licenses and support has been bought from third-party vendors which include telephone systems and cloud services. Likewise, a few other PaaS solutions has been integrated that were developed by a third-party vendor. Technical hardware has been supplied, and information systems developed and maintained by third-parties. These are the examples of services that are being outsourced. Outsourcing as a business process is described in the next sections.

## 3.2 Outsourcing System and Its Components

Outsourcing is the relationship between the outsourcing entity and the external third-party to provide services and solutions that otherwise would be provided by the outsourcing entity itself. For the upcoming information security risk analysis, the outsourcing system is defined as the collection of the following components:

1) Organization employees who are responsible for conducting one or many tasks in the context of outsourcing, such as project manager, contract owner, human resources representative, IT specialist, information security manager, purchase committee, legal counsel, operational risk manager, compliance manager, etc.;
2) external parties who provide services, or monitor legal and regulatory compliance, or protect the interests of employees, such as service providers, Financial Stability Authority (FSA), unions;
3) the infrastructure needed for the communication of the parties, such as email service;
4) the infrastructure needed to store information, such as contract storage management system, and document database;
5) the information that is exchanged between parties, such as outsourcing agreement, risk assessment plan, and many more.

The overall system of outsourcing is relatively complex. It needs the involvement, collaboration, and communication of a significant number of parties, which is supported by relevant infrastructure needs and application.

## 3.3 Security Objectives of Outsourcing

The focus of the thesis is on information security and the importance of maintaining it in the context of third-party outsourcing. Information security objectives that need to be ensured are described as follows:

- *Confidentiality* is maintained when data is protected from unauthorized access.
- *Integrity* is maintained when data is accurate, not modified or altered.
- *Availability* is maintained when access to data for authorized persons is assured.

These three objectives are the most common ones that are used. The financial institution has no exceptional views in this case.

## 3.4 Outsourcing Business Process

The overall business process of outsourcing is illustrated in Figure 5. It is divided into five phases, which vary in the amount and complexity of tasks. An overview with a less detailed insight into the phases is described in the following paragraphs.

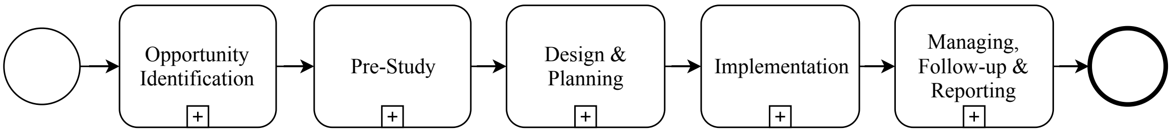


Figure 5. Outsourcing phases

Opportunity Identification is the first phase during which the initial steps are taken to estimate the outsourcing opportunities. A Project manager creates the *scope* of outsourcing, starts its review and forwards it to the legal counsel. The legal counsel reviews the *scope*, decides on its applicability and whether to notify the FSA. If needed, then the FSA is contacted. The FSA forms their *response* and sends it to the legal counsel who forwards the overall *applicability* answer to the project manager. If the *scope* is denied, then the project manager should renew it. If the *scope* is applicable, then an indicative *project plan* and the *business case* should be created. The project manager also develops an initial *risk assessment* and submits a *new product approval process* initiation. The last two documents are shared with the operational risk or information security manager.

Pre-Study is the second phase during which a high-level solution for outsourcing is created. The project manager sends *information* to the human resources about the upcoming outsourcing. The human resources decide whether to inform the unions about it. If it is decided to inform the unions, then *information* is sent to them. The project manager also submits a *purchase request* and the purchase committee decides whether to proceed or not. If the *purchase request* is approved, then the project manager identifies the *application inventory* and defines *development needs*. Support should be asked from the system owner or information security manager. Also, the project manager updates the previously created documents.

Design & Planning is the third phase, which is divided into the process design phase and service provider phase. Process design phase aims for developing a detailed solution for outsourcing. In this phase, the project manager starts drafting the *outsourcing agreement* together with the legal counsel. Also, the project manager creates the *internal exit and business continuity management plan*. This is done together with the support from the operational risk manager. Furthermore, the project manager creates the *communication plans* together with the compliance manager that describes if and how the communication with FSA will be managed. Also, the project manager updates the previously created documents. Service provider phase is important to analyse possible service providers and prepare for the next phase. The project manager analyses the possible service providers and sends the purchaser the *outsourcing agreement*. The purchaser contacts the service providers and introduces the *outsourcing agreement* to them. Selection of the service provider is made. In case of in-house outsourcing, then the project manager forwards *legal documents* to the entity representative who signs them. Also, the project manager creates the initial *value realisation measurement plan* which estimates the financial outcome and lists the key employees related to the outsourcing. Also, the previously created documents are updated.

Implementation is the fourth phase during which the *outsourcing agreement* is signed, and the overall outsourcing process is implemented. This phase has been used in the analysis part of the thesis to conduct the information security risk assessment using ISSRM and BNBAG methods. The reason is that it has various information system components represented and is important in the context of outsourcing. It is divided into sub-processes that are described in Section 3.5.

Managing, Follow-up & Reporting is the last phase of outsourcing. It describes the after actions and follow-up activities when the *outsourcing agreement* has been signed and the chosen service provider has started providing the required services and solutions for the outsourcing entity. The project manager monitors the financial outcomes and documents relevant feedback, updates *value realisation* and creates *key learnings*. The contract owner monitors *contract fulfilment* and the *performance of the service provider*. Also, the contract owner is responsible for monitoring *risk management & mitigation* and *internal exit and business continuity management plan*. The contract owner has to evaluate the economic viability of the service provider. The register owner compiles *outsourcing reports* at least yearly to follow-up on contract fulfilment, service provider's financial status, critical incidents, risks, and related action plans. These reports are stored in a document database which is accessible for the authorized parties. There five phases together form the outsourcing business process.

## 3.5 Assets in Outsourcing System

The system components of outsourcing have been introduced in Section 3.2 and an overview of the phases of outsourcing has been described in Section 3.4. For further discussion, only the fourth phase – implementation – is considered in the analysis. It represents important internal and external communicating parties, infrastructure needs for communication and storage, and information that flows through the system.

The upcoming implementation phase process description is based on the financial institution's internal handbook of outsourcing. The accuracy of the information flow, communicating parties, the information system, and business assets has been verified by the responsible person from the financial institution. The business process modelling notation (BPMN) based process graphs have been compiled by the author. Open software, draw.io, has been used to model the business processes. To make the analysis easier to follow, the implementation has been divided into four phases which order is illustrated in Figure 6.

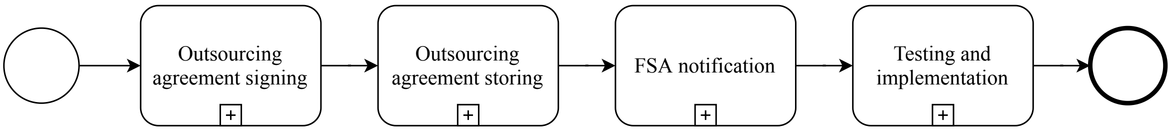

Outsourcing agreement signing
Outsourcing agreement storing
FSA notification
Testing and implementation

Figure 6. Implementation phases

The first phase, the outsourcing agreement signing, is detailed in Figure 7. and Figure 8. The following steps describe the business process of outsourcing agreement signing by the project manager, described in Figure 7.

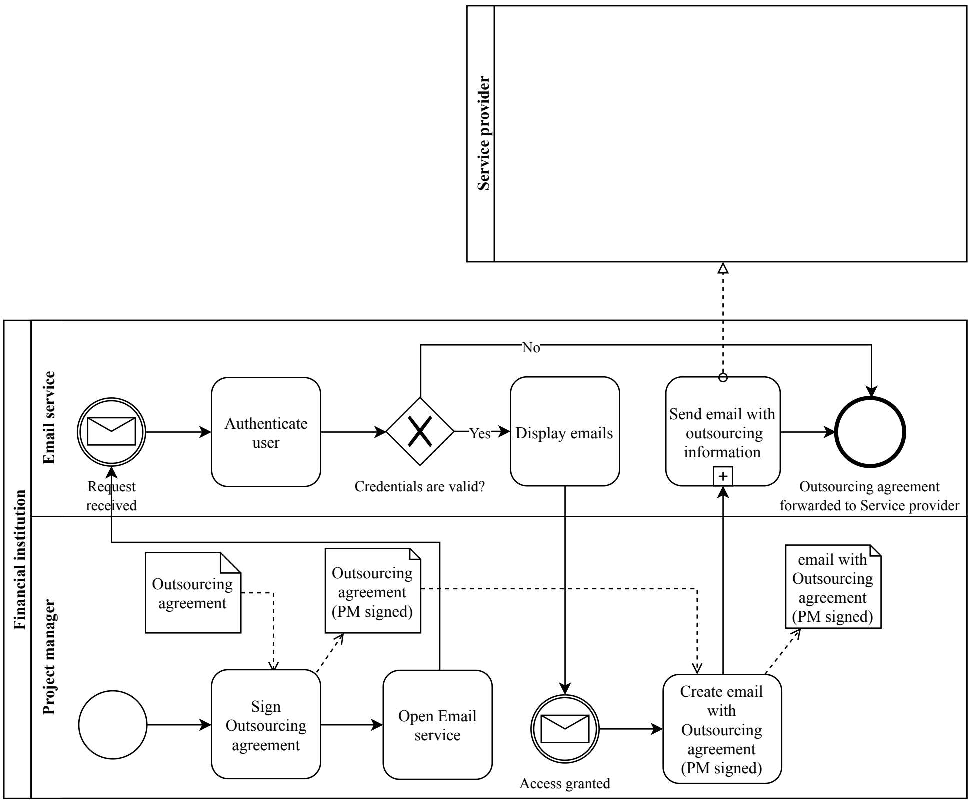

Service provider
Financial institution
Email service
Project manager
Request received
Authenticate user
Credentials are valid?
No
Yes
Display emails
Send email with outsourcing information
Outsourcing agreement forwarded to Service provider
Outsourcing agreement
Outsourcing agreement (PM signed)
email with Outsourcing agreement (PM signed)
Sign Outsourcing agreement
Open Email service
Access granted
Create email with Outsourcing agreement (PM signed)

Figure 7. Outsourcing agreement signed by project manager

Project manager (PM) *signs outsourcing agreement* and project manager *opens email service*. Email service *receives a request* and *authenticates the user*. If credentials are valid, then *emails* will be *displayed*. If credentials are not valid, then access to email service will not be granted. Project manager *creates an email with the outsourcing agreement (PM signed)*. Email service *sends the email with outsourcing agreement (PM signed)* to the service provider.

The following steps describe the flow of the outsourcing agreement, signed by both parties, back to the project manager. It is illustrated in Figure 8. Email service *receives the email with outsourcing agreement (signed)*, *stores* it and *notifies email recipient*. Project manager *receives notification* and *opens email service*. Email service *receives a request* and *authenticates the user*. If credentials are valid, then *a download of the email* will be allowed. If credentials are not valid, then a download of the email will not be allowed. Project manager *downloads email with outsourcing agreement (signed)*. Outsourcing agreement is signed by both parties.

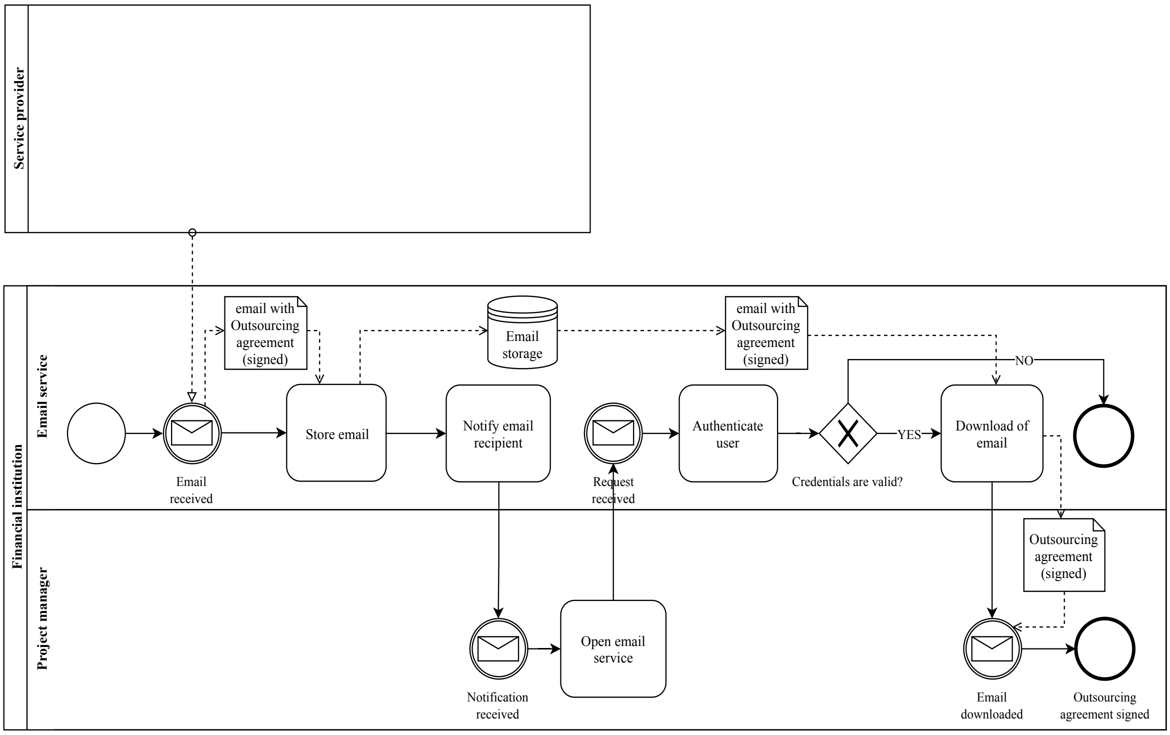


Figure 8. Outsourcing agreement signed by both parties

The second phase of implementation is outsourcing agreement storing which is presented in Figure 9. An email sending process is the same, therefore, it is not illustrated in the figure. The following steps describe the outsourcing agreement storing.

Contract owner *receives an email with outsourcing agreement (signed) and support materials*. Contract owner *opens the contract management system*. The contract management system *receives an access request* and *authenticates the user*. If credentials are valid, then *permissions to access system* will be *checked*. If credentials are not valid, then contract management system *logs failed login attempt*. If permissions are valid, then *access will be granted*. If permissions are not valid, then access will not be granted. Contract owner *inputs outsourcing agreement (signed)* to the contract management system. The contract management system *receives a request* and *validates user input*. If the user input is valid, then *outsourcing agreement (signed)* will be *processed*. If the user input is not valid, the process stops. Contract management system *stores outsourcing agreement (signed)* and *notifies* contract owner. Contract owner *receives a notification*.

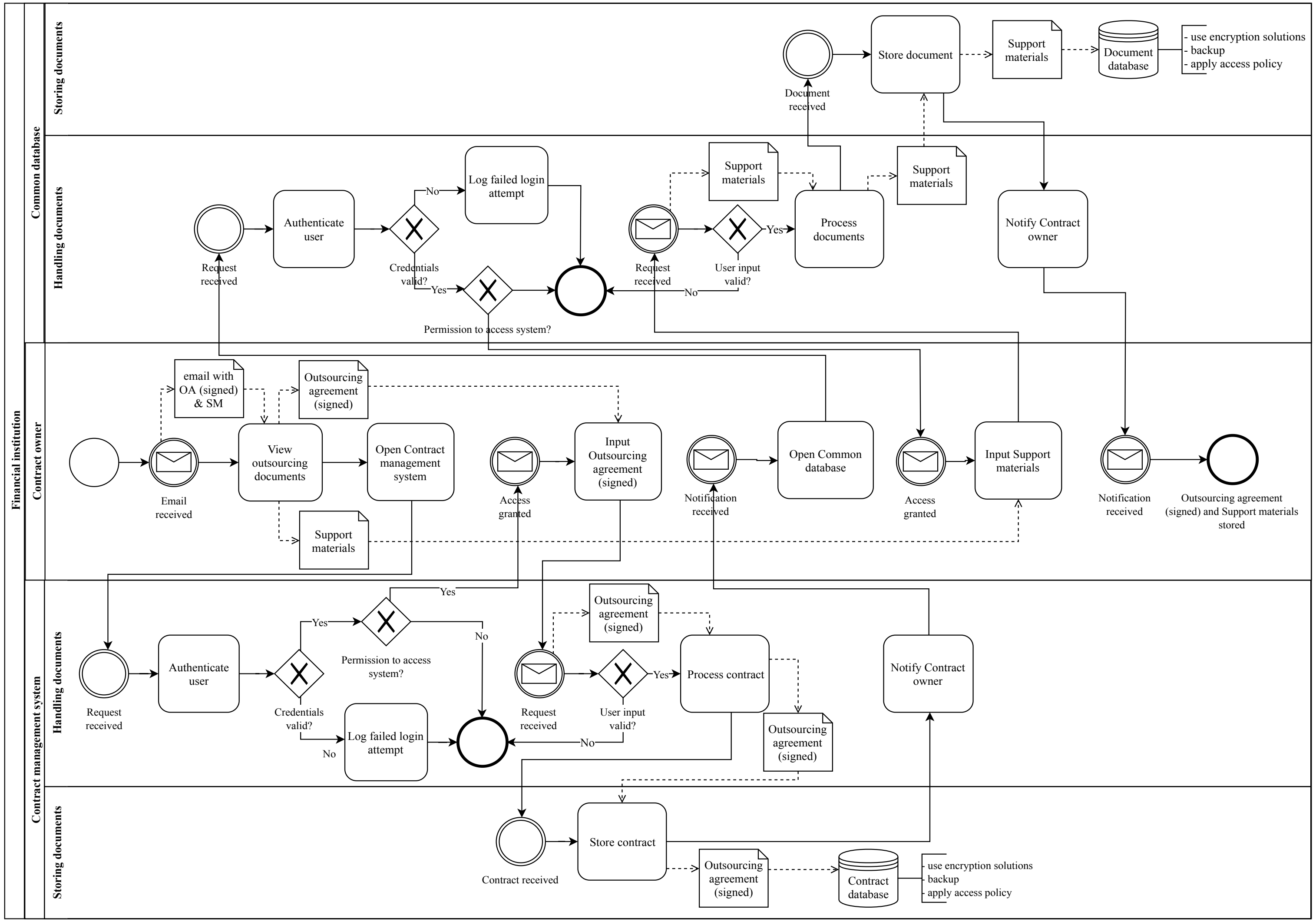


Figure 9. Outsourcing agreement storing

Contract owner *opens the common database*. The common database *receives an access request* and *authenticates the user*. If credentials are valid, then *permissions to access system* will be *checked*. If credentials are not valid, then contract management system *logs failed login attempt*. If permissions are valid, then *access* will be *granted*. If permissions are not valid, then access will not be granted. Contract owner *inputs support materials*. The common database *receives a request* and *validates the user input*. If the user input is valid, then *support materials will be processed*. If the user input is not valid, the process stops. The common database *stores support materials* and *notifies contract owner*. Contract owner *receives notification*. Outsourcing agreement (signed) and support materials are stored.

The third phase of implementation is FSA notification phase, which is illustrated in Figure 10. and the following steps are taken to complete the phase. Compliance representative *signs FSA application* and *opens email service*. Email service *receives a request* and *authenticates the user*. If credentials are valid, then *emails will be displayed*. If credentials are not valid, then access to email service will not be granted. Compliance representative *creates an email with FSA application (signed)*. Email service *sends the email with FSA application (signed)*. FSA is notified.

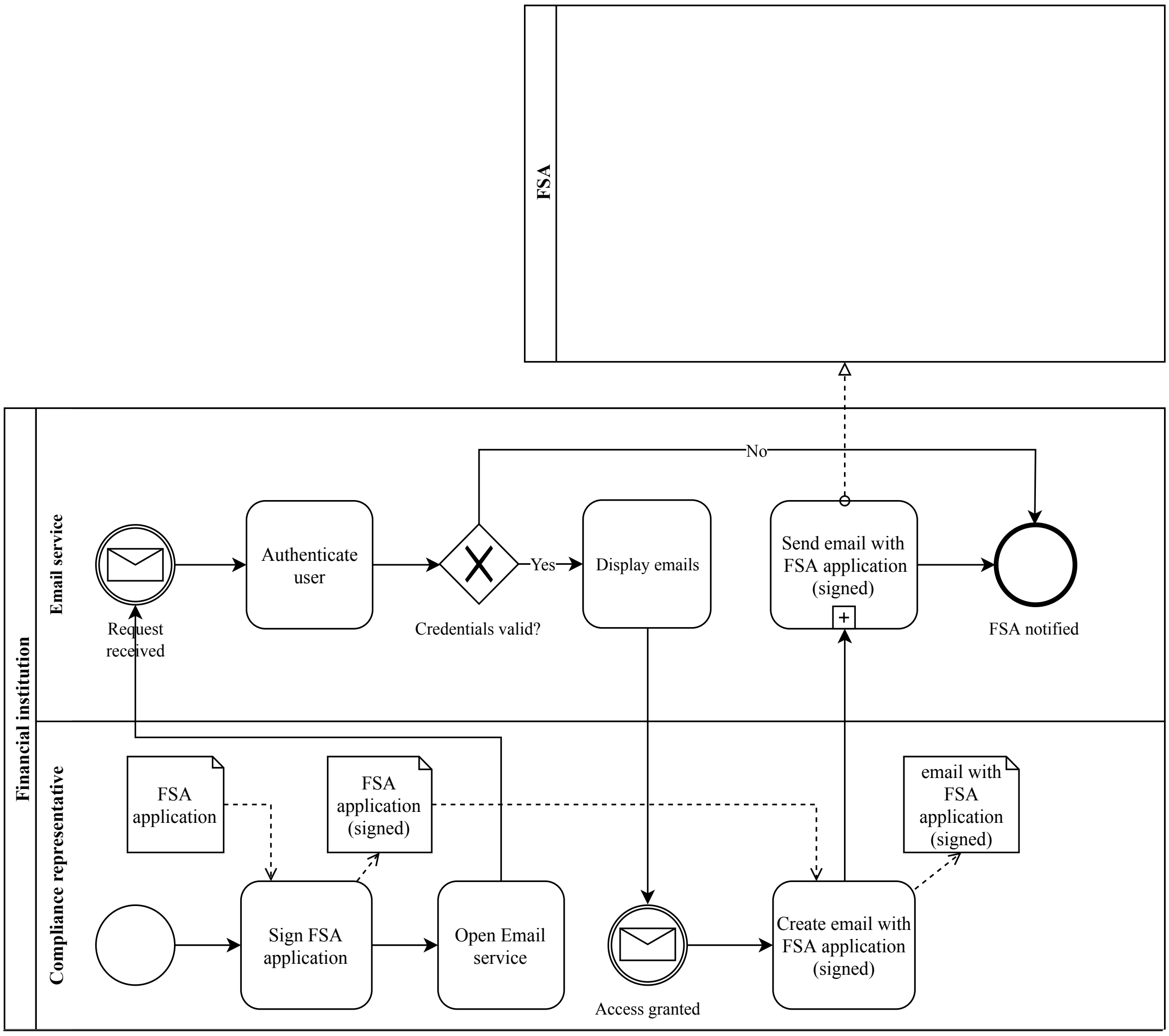


Figure 10. FSA notification

The fourth phase of implementation is testing and implementation, which is illustrated in Figure 11., to give a complete overview of the business process of implementation. The financial institution's outsourcing handbook has not covered it in detail; hence, it is presented here simply as tasks that the project manager is responsible for conducting. During this phase, the project manager is responsible for the following *ensuring that applications are tested* in a production environment. (S)he *executes the implementation of the outsourcing scope* and *updates the value realisation measurement plan*.

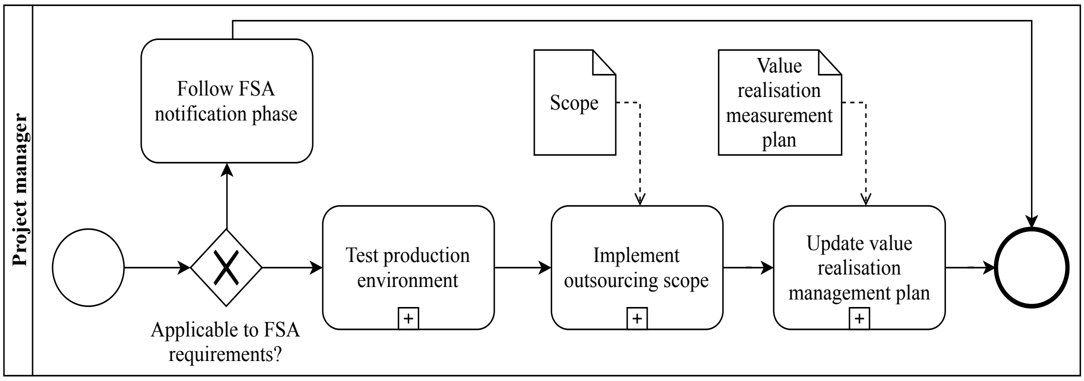

Project manager
Follow FSA notification phase
Scope
Value realisation measurement plan
Applicable to FSA requirements?
Test production environment
Implement outsourcing scope
Update value realisation management plan

Figure 11. Testing and implementation

These four phases form the implementation phase of outsourcing. In this chapter, the outsourcing business process has been introduced. The described business process will be used in the upcoming chapters.

## 3.6 Chapter Summary

The chapter has given a description of the case study. An overview of outsourcing in the context of the financial institution has been given, emphasizing the opportunities and risks that characterize outsourcing. Third-party outsourcing has been marked as one of the top challenges in the financial sector.

The outsourcing system and its components have been introduced in the context of the financial institution. The overall outsourcing process has been described. It consists of the following five stages: *opportunity identification*, *pre-study*, *design and planning*, *implementation*, and *managing, follow-up, and reporting*. To narrow the scope of risk assessment, the *implementation* stage has been chosen for further analysis as it represents both internal and external communicating parties, information systems that are used to exchange information and store it. The process has been divided into four phases: *outsourcing agreement signing*, *outsourcing agreement storing*, *FSA notification*, and *testing and implementation*. These processes have been illustrated using BPMN modelling language.

The description and visualization of the phases of implementation have been used to identify the business and information system assets which are relevant for assessing information security risk in the following chapter.

# 4 Information Security Risk Assessment Using ISSRM

The upcoming chapter follows the ISSRM domain model, illustrated in Figure 1., to identify information security risk scenarios in the implementation phase of outsourcing. Information security risk assessment process starts with identifying the business and information system assets. From this implementation use case, the system assets that support the business assets are the following:

1. Internal parties: project manager, contract owner, compliance representative.
2. External parties: service provider, FSA.
3. Infrastructure and services: email service
4. Applications/components to support activities: Contract management system, Common database, Email storage, Contract database, Document database.

The main business assets in the implementation phase are the following:

1. Outsourcing agreement
2. Support materials
3. FSA application

In this chapter, the threats and vulnerabilities of the information system have been identified. Potential risk scenarios have been created using the potential threats that could exploit the vulnerabilities leading to an impact on the financial institution. The result of the information security risk assessment has been presented as the list of prioritized risk scenarios.

## 4.1 Threats in Outsourcing System Using ISSRM

According to the ISSRM domain model, illustrated in Figure 1., a threat is a threat agent who uses an attack method to exploit a vulnerability of the information system asset. According to the ENISA report [38] and the information from the financial institution, the dominating adversarial threat agents are criminal groups and nation states. Accidental threat agent could be an internal employee either with privileged access to systems or without any. Also, an accidental threat agent could be an employee of a partner or vendor with access to systems or data.

According to the research by ENISA and Europol [38] [39] and the information from the financial institution, the following attack methods are most commonly used by the threat agents. Spreading malware is the leading attack method in all industries. What is more financial sector-specific malware, is the high number of reported banking Trojans and ransomware Trojans. Also, the number of attack methods using social engineering techniques have risen and established themselves as effective methods for infecting the information systems. Distributed Denial of Service (DDoS) is still aimed for targeting the availability of systems. Also, fraud attacks, information thefts and data breaches are notable threats that financial institutions face.

In the implementation phase of outsourcing, all the named threat agents can potentially use the described attack methods to exploit one or more vulnerabilities. The selection of a suitable attack method has been made depending on the existing vulnerabilities in the system. ENISA threat taxonomy [24], described in the theoretical chapter, has been used to classify threats. The considered attack vectors fall under the categories of nefarious activity and interception: injection attack, unauthorized access, hijacking, unauthorized use of IS, misuse of IS, Phishing, Malicious software, and information gathering. The relevant threat agents and common attack methods have been introduced.

## 4.2 Vulnerabilities in Outsourcing System Using ISSRM

An overview of the information flow in the implementation phase of the outsourcing system has been introduced. Information is transmitted through information system assets. Following the ISSRM domain model, vulnerabilities are the characteristics of the defined information system assets which could be exploited by a threat. OWASP Top 10 taxonomy [27] has been used to characterize the vulnerabilities. The vulnerability classes in OWASP Top 10 are reflected in the implementation phase in a way that is presented in Table 5. The reason for using OWASP Top 10 has been explained in the theoretical chapter.

Table 5. Vulnerabilities in implementation phase for ISSRM analysis

| OWASP category | Vulnerability ID | Vulnerability in implementation phase | Targeted information system asset |
|---|---|---|---|
| Injection | CWE89 | Improper neutralization of special elements used in an SQL command in database servers | Contract management system or Common database |
| Broken authentication | CWE287 | Improper authentication in Email service | Email service |
| Sensitive data exposure | CWE319 | Cleartext transmission of sensitive information between user and Email service | Email service |
| XXE | CWE611 | - | - |
| Broken access control | CWE285 | Improper authorization in databases | Contract database or Document database |
| Security misconfiguration | CWE16 | Lack of appropriate access control implementation in databases | Contract database or Document database |
| Cross-site scripting | CWE79 | Improper neutralization of input during web page generation in database servers | Contract management system or Common database |
| Insecure deserialization | CWE502 | - | - |
| Using components with known vulnerabilities | CWE937 | Existence of known unpatched vulnerabilities in database servers | Contract management system or Common database |
| Insufficient logging and monitoring | CWE778 | Insufficient logging of failed login attempts in database servers | Contract management system or Common database |

Source: Compiled by the author (based on OWASP Top 10 data [40])

Notes: 1) the symbol “-“ indicates that these vulnerabilities have not been included in the analysis as they are not present in the system.

The Table 5. introduces the sample of vulnerabilities as the characteristics of information system assets. Depending on the evaluation, there could be additional vulnerabilities found in the implementation phase of the outsourcing system.

## 4.3 Impact in Outsourcing System Using ISSRM

According to the ISSRM domain model, illustrated in Figure 1., when a threat agent with an attack method successfully exploits one or more vulnerabilities in a system, it will lead to an impact that harms an asset and negates the security criterion. Table 6. represents eight potential risk scenarios of the implementation phase of outsourcing where a threat agent with an attack method successfully exploits a vulnerability which leads to an impact. The threats have been categorized according to ENISA taxonomy [24], which has been introduced in the theoretical chapter.

Table 6. Threats, vulnerabilities and impact for ISSRM analysis

| Threat | Risk scenario |
|---|---|
| Injection attack | ***Threat***: An attacker with a motivation to read Outsourcing agreement from Contract database and Support materials from Common database by sending crafted SQL injection statements though Contract management system or Common database.<br>Attack method:<br>1. Access Contract management system or Common database application.<br>2. Identify the non-validated user input field.<br>3. Send crafted SQL injection statements through the application.<br>4. Gain access to data.<br>***CWE89***: Improper neutralization of special elements used in an SQL command in database servers.<br>***Impact***: Loss of confidentiality of Outsourcing agreement and Support materials. |
| Unauthorized access to IS | ***Threat***: An attacker with a motivation to gain access to Outsourcing agreement in Email server by using keylogger to obtain the user's password associated with the smartcard and stealing the smartcard.<br>Attack method:<br>1. Use keylogger to obtain password associated with the smartcard of a user.<br>2. Steal the smartcard.<br>3. Use the stolen smartcard and its password to connect to the network.<br>4. Gain access to Email service.<br>***CWE287***: Improper authentication in Email service.<br>***Impact***: Loss of confidentiality of Outsourcing agreement. |

| | |
|---|---|
| Hijacking | ***Threat***: An attacker with a motivation to alter the transported Outsourcing agreement by using the same network as the user, sniffing and capturing the session token.<br>Attack method:<br>1. Use the same network.<br>2. Sniff traffic for session token in unencrypted traffic.<br>3. Capture the session token.<br>4. Alter the transported data.<br>***CWE319***: Cleartext transmission of sensitive information between user and Email service.<br>***Impact***: Loss of confidentiality of Outsourcing agreement. |
| Unauthorized use of software | ***Threat***: An attacker with a motivation to get Outsourcing agreement and Support materials from databases by running an arbitrary SQL query on databases without being authorized to do it and receiving Outsourcing agreement and Support materials as the result of the query.<br>Attack method:<br>1. Become authenticated user in the system.<br>2. Run arbitrary SQL query on Contract database or Common database without being authorized to do it.<br>3. Receive the result of the query.<br>4. Obtain Outsourcing agreement and Support materials from databases.<br>***CWE285***: Improper authorization in databases.<br>***Impact***: Loss of confidentiality of Outsourcing agreement and Support materials. |
| Misuse of IS | ***Threat***: An attacker with a motivation to get Outsourcing agreement from Contract database and Support materials from Common database by having knowledge about the misconfigured databases and misusing the legitimately-assigned access rights.<br>Attack method:<br>1. Have knowledge about user access rights being misconfigured in Contract database or Common database.<br>2. Exploit user access rights misconfiguration in Contract database or Common database.<br>3. Misuse legitimately-assigned access rights to access document in database.<br>***CWE16***: Lack of appropriate access control implementation in databases.<br>***Impact***: Loss of confidentiality of Outsourcing agreement and Support materials. |

| | |
|---|---|
| Phishing | ***Threat***: An attacker with a motivation to exfiltrate sensitive information from Contract management system and Common database by embedding a malicious script in URL and sending it as a phishing email to a target user.<br>Attack method:<br>1. Craft a malicious script and embed it in HTTP request.<br>2. Send phishing email to a user containing the URL.<br>3. Receive a response from application after the user has clicked on the malicious URL.<br>***CWE79***: Improper neutralization of input during web page generation in database applications.<br>***Impact***: Loss of confidentiality of Contract management system and Common database. |
| Malicious software | ***Threat***: An attacker with a motivation to read and modify Outsourcing agreement and Support materials by crafting a malware to exploit known unpatched vulnerabilities.<br>Attack method:<br>1. Have knowledge about the unpatched vulnerabilities in Contract management system or Common database.<br>2. Craft a malware to exploit the vulnerabilities.<br>3. Gain access to Contract database or Document database.<br>4. Read and modify Outsourcing agreement and Support materials.<br>***CWE937***: Existence of known unpatched vulnerabilities in database servers.<br>***Impact***: Loss of confidentiality and integrity of Outsourcing agreement and Support materials. |
| Information gathering | ***Threat***: An attacker with a motivation to gather Outsourcing agreement and Support materials by developing attack vectors to target database information without leaving any trail for forensic analysis.<br>Attack method:<br>1. Have knowledge about incomplete recording of events.<br>2. Perform unauthorized scanning of information systems.<br>3. Develop attack vectors to attack database information without any trail for forensic analysis.<br>4. Gather Outsourcing agreement and Support materials.<br>***CWE778***: Insufficient logging of failed login attempts in database servers.<br>***Impact***: Loss of confidentiality of Outsourcing agreement and Support materials. |

Source: Compiled by the author

These scenarios are based on subjective estimation by the author. Scenario modelling is important to illustrate the potential attack vectors that a threat agent could deploy to exploit the vulnerabilities in the system leading to a certain impact.

The architecture and design of the information systems of the financial institution are complex; hence it is difficult to propose potential attack vectors to target vulnerabilities in the system. Financial institutions have to be compliant with requirements, e.g. MiFID [36] and PSD2 [37]. Targeting the unregulated service provider whose systems are highly integrated with the financial institution could result in a greater impact on the financial institution. Despite the contrary, the service provider side of the analysis has been left out due to the lack of knowledge of the service provider's information system architecture, the integration between the systems and the information flow.

## 4.4 Information Security Risks in Outsourcing System Using ISSRM

Risks are important to assess to have the basis for making decisions about possible treatment options or controls selection. Financial sector institutions are obligated to assess their risks to be compliant with laws and regulations. According to the ISSRM domain model, risk is the combination of a threat event and its caused impact. All the defined scenarios of the implementation phase presented in Table 6. are evaluated using ISSRM metrics and the results are presented in Table 7.

Table 7. Risk level for ISSRM analysis

<table>
<tr><th>Threat</th><th colspan="2">Business asset</th><th colspan="5">Risk description</th></tr>
<tr><td rowspan="4">Injection attack</td><td colspan="2">Outsourcing agreement and Support materials</td><td colspan="5">An attacker with a motivation to read Outsourcing agreement from Contract database and Support materials from Common database by sending crafted SQL injection statements though Contract management system or Common database due to improper neutralization of special elements used in an SQL command in database servers lead to loss of confidentiality of Outsourcing agreement and Support materials.</td></tr>
<tr><td rowspan="2">Business asset value</td><td colspan="6"><b>Risk level calculation</b></td></tr>
<tr><td>Security need</td><td>Threat likelihood</td><td>Vulnerability level</td><td>Potentiality</td><td>Impact</td><td>Risk level</td></tr>
<tr><td>3</td><td>C 3<br>I 2<br>A 1</td><td>3</td><td>2.5</td><td>4.5</td><td>3</td><td>13.5</td></tr>
<tr><td>Unauthorized access to IS</td><td>3</td><td>3</td><td>1</td><td>2</td><td>2</td><td>3</td><td>6</td></tr>
<tr><td>Hijacking</td><td>3</td><td>3</td><td>2</td><td>2.5</td><td>3.5</td><td>3</td><td>10.5</td></tr>
<tr><td>Unauthorized use of software</td><td>3</td><td>3</td><td>2</td><td>2</td><td>3</td><td>3</td><td>9</td></tr>
<tr><td>Misuse of IS</td><td>3</td><td>3</td><td>2</td><td>3</td><td>4</td><td>3</td><td>12</td></tr>
<tr><td>Phishing</td><td>3</td><td>3</td><td>3</td><td>3</td><td>5</td><td>3</td><td>15</td></tr>
<tr><td>Malicious software</td><td>3</td><td>3</td><td>3</td><td>3.5</td><td>4.5</td><td>3</td><td>13.5</td></tr>
<tr><td>Information gathering</td><td>3</td><td>3</td><td>2</td><td>2</td><td>3</td><td>3</td><td>9</td></tr>
</table>

Source: Compiled by the author (using ISSRM metrics [8])

There are seven metrics that are defined to calculate the risk level of a threat successfully exploiting one or more vulnerabilities leading to an impact on the organization. The security need is evaluated as high level of need for confidentiality or integrity or available for all business assets, which also indicates that the impact is evaluated to be with the same value following the calculation rules of the ISSRM method. Threat likelihood is based on the subjective judgement about the attacker's motivation and the sophistication level of the attack. The vulnerability level is evaluated as the average of the prevalence value and detectability value of the vulnerability based on OWASP evaluation [27]. Other metrics are calculated using the equations introduced in the theoretical chapter of the thesis.

These risk scenarios can be prioritized according to their risk level which indicates the criticality level of the risk for the organization and business asset value. As can be seen, the business asset value is considered to be high in all risk scenarios. Also, there are a number of attacks which are calculated to have the same risk level. Hence, the decision to start risk treatment from the most critical one is difficult. However, risks can be prioritized into the following list based on the risk level in Table 7.:

1. Phishing
2. Injection attack, Malicious software
3. Misuse of information system
4. Hijacking
5. Unauthorized use of software, Information gathering
6. Unauthorized access to information systems

The topic of the thesis is information security risk assessment which consists of identifying, analysing and evaluating the risks. ISSRM is a risk management method which includes risk treatment and controls as part of the whole process. Following the illustration of ISSRM process, the risk assessment process consists of (a) context and asset identification, (b) security objectives determination, and (c) risk analysis and assessment. Hence, the other parts of ISSRM are not analysed due to the limited scope of the research work.

## 4.5 Chapter Summary

An overview of information security risk assessment using ISSRM method has been given in this chapter. Firstly, the relevant assets of the implementation phase of outsourcing have been introduced. Both the business assets as well as the supporting information system assets have been listed. The potential threats which are described as a threat agent with an attack method have been described. ENISA threat taxonomy [24] has been used to make the threat analysis consistent with existing practises of the financial institution. As the following step, the vulnerabilities which are the characteristics of the information system assets have been identified. OWASP Top 10 vulnerability taxonomy [27] has been used because it has been used in the financial institution before. After the vulnerabilities and threats have been described, eight risk scenarios have been represented adding the potential impact on the organization. The risk assessment results have been presented in Table 7. The scenarios have been prioritized according to the risk level which has been calculated using the ISSRM metrics. Overall, an illustration of how risk assessment can be done on the implementation phase with ISSRM method has been included in this chapter.

# 5 Information Security Risk Assessment Using BNBAG

The BNBAG method [9] [10] is a probabilistic risk assessment method. It has been introduced in Section 2.3. The next sections follow the steps of BNBAG process shown in Figure 4: (i) identifying the vulnerabilities of the outsourcing system; (ii) illustrating the dependencies between vulnerabilities; (iii) calculating the NPTs, and (iv) evaluation of attack probability.

## 5.1 Identification of Vulnerabilities in Outsourcing System Using BNBAG

The BNBAG method [9] [10] is a vulnerability-related risk assessment method. Vulnerabilities are the weaknesses in the system that can be exploited by an adversary. A sample of vulnerabilities that have been used in ISSRM have been chosen for BNBAG analysis: Improper neutralization of special elements used in an SQL command (CWE89), improper authentication (CWE287), cleartext transmission of sensitive information (CWE319), broken authorization (CWE285), misconfiguration of access controls (CWE16), improper neutralization of input during web page generation (CWE79), existence of known unpatched vulnerabilities (CWE937), and insufficient logging of failed login attempts (CWE778). Overview of the data is presented in Appendix I. All of them can be found in the implementation phase of the outsourcing system. Additional information about the vulnerabilities is available on the MITRE CWE webpage [41].

BNBAG method enables modelling dependencies between vulnerabilities. While many different dependencies can be present in the system, the following limited list of dependences have been chosen for current example analysis:

1. CWE287 and CWE89 – improper authentication can depend on a successful exploit of SQL injection vulnerabilities [42].
2. CWE285 and CWE16 – improper authorization can depend on misconfiguration of access controls implemented in IS.

In the analysis, the probability of a successful attack by an exploit of independent vulnerability is defined as the product of the *probability of finding the vulnerability in the system* and the *likelihood of its exploit*. Publicly available data provided by the OWASP Project [40] is used in the analysis for the average estimation of the probability *of finding the vulnerability in the system*. The description of the data is presented in Appendix I and Appendix II. CWE list is used to estimate the *likelihood of the exploit of a vulnerability* [41]. CWE list describes the likelihood of exploit using low/medium/high, which match the numbers 0.2/0.6/1.0. It has been added to the data presented in Appendix I.

## 5.2 Attack Graph in Outsourcing System Using BNBAG

The selection of identified vulnerabilities and their dependences, as described in Section 5.1 are used to build an example attack graph shown in Figure 12.[1] The attack graph is an illustrative example, which enables to demonstrate how dependencies between vulnerabilities can be modelled during risk assessment.

In the following analysis, an *incident* is defined as the potential compromise of confidentiality, integrity, or availability, which is a common definition of an information security incident in the financial industry. An *incident* in BNBAG method is an *event* in ISSRM method. Attack graph in Figure 12. shows all considered attack vectors, which can be used to cause an incident. Firstly, the vulnerabilities can be targeted independently for a

[1] It is done in RStudio using R which script has been added in Appendix III.

successful incident to occur. Secondly, the exploit of one vulnerability can increase the probability of exploit of another vulnerability with dependency, meaning that the second vulnerability's potential exploit depends on the success of the previous one. This situation is illustrated with dependence between vulnerabilities CWE285 and CWE16, and dependence between vulnerabilities CWE287 with CWE89.

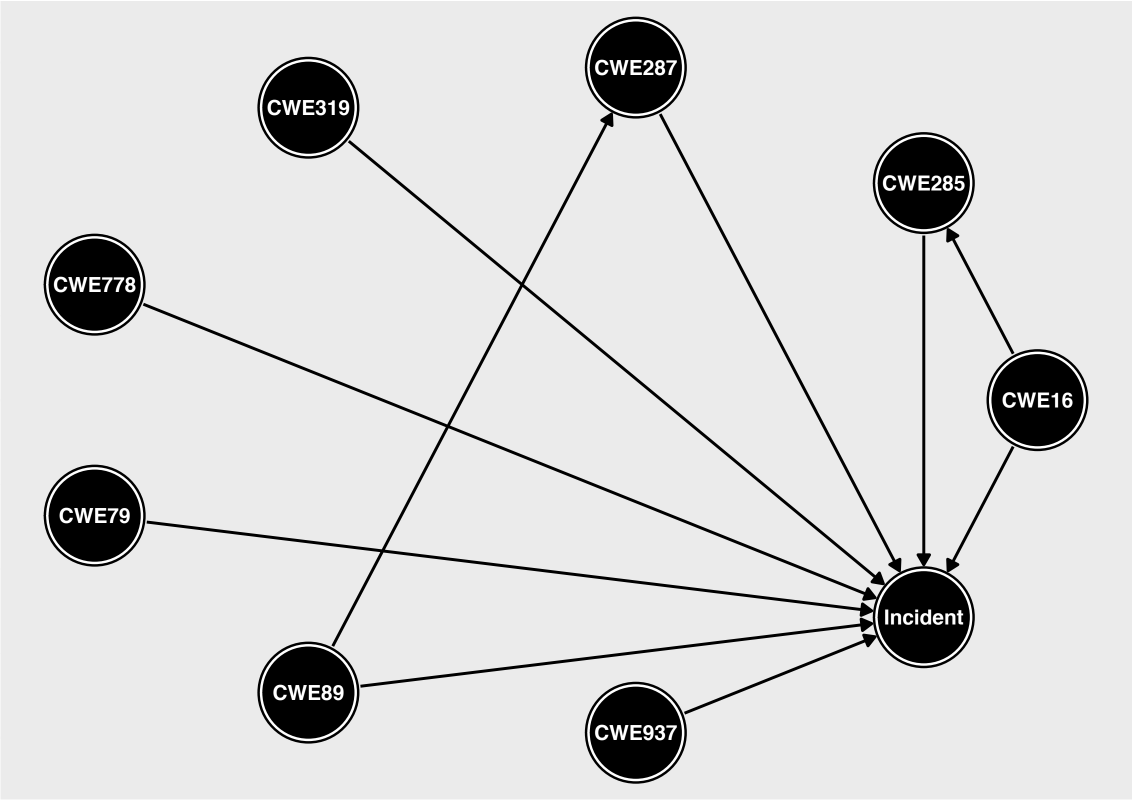


Figure 12. Attack graph modelling a set of selected vulnerabilities for BNBAG analysis

It is possible to target vulnerabilities independently. Also, it is possible to use an attack vector which successfully exploits one vulnerability node enabling the attacker to exploit also the dependent vulnerability. In Section 5.3, node probability tables are formed to illustrate the calculation of the joint probability of an incident, taking into consideration the dependencies between different vulnerability nodes.

## 5.3 Node Probability Tables in Outsourcing System Using BNBAG

NPTs provide input for computing the overall probability of a successful incident. NPTs for independent and dependent vulnerabilities are presented in Table 8. The *true (T)* value represents the probability of an occurrence of an exploit of a certain vulnerability. It is calculated as the probability of the vulnerability being present in the system multiplied with its likelihood of exploit. The *false (F)* value represents the probability of non-occurrence of such event. As the probability of the *false (F)* value represents the probability of the complement of occurrence, then it is calculated as one minus the probability of the occurrence of an exploit.

NPTs for all of the identified vulnerabilities are provided in Table 8. including the conditional probabilities of the vulnerabilities CWE285 and CWE287. The probabilities of CWE285 and CWE287 indicate their potential dependence on the existence of vulnerabilities CWE16 or CWE89 in the system. Firstly, NPT for CWE285 given CWE16 indicates that the probability of CWE285 is *true* given that CWE16 is *true* with a value of 0.15 based on subjective input. This means that if the access controls have been misconfigured, then there is a probability that the user is improperly authorized. The probability that CWE is *true* given that CWE16 is *false* is 0.02, i.e. the independent probability of CWE285 which is calculated from data. Secondly, NPT for CWE287 given CWE89 is represented. The probability that CWE287 is *true* given that CWE89 is *true* is 0.09. This value is based on subjective input. The probability that CWE287 is *true* given that CWE89 is *false* is 0.04, i.e. the independent probability of the vulnerability CWE287.

Table 8. NPTs of vulnerabilities for BNBAG analysis

| NPT | **CWE16** |
|---|---|
| T | 0.24 |
| F | 0.76 |

| NPT | **CWE89** |
|---|---|
| T | 0.10 |
| F | 0.90 |

| NPT | **CWE319** |
|---|---|
| T | 0.05 |
| F | 0.95 |

| NPT | **CWE79** |
|---|---|
| T | 0.24 |
| F | 0.76 |

| NPT | **CWE937** |
|---|---|
| T | 0.01 |
| F | 0.99 |

| NPT | **CWE778** |
|---|---|
| T | 0.00(1) |
| F | 0.99(9) |

| NPT | CWE16 | |
|---|---|---|
| **CWE285** | T | F |
| T | 0.15 | 0.02 |
| F | 0.85 | 0.98 |

| NPT | CWE89 | |
|---|---|---|
| **CWE287** | T | F |
| T | 0.09 | 0.04 |
| F | 0.91 | 0.96 |

Source: Compiled by the author (based on OWASP data [40] and MITRE evaluation [41])

Node probabilities of dependent variables are calculated using Equation 4. for prior marginal probability calculation. Firstly, CWE285 is dependent on CWE16 as shown by the attack graph in Figure 12. The probability of a successful attack via vulnerability CWE285 is computed for CWE16 being either *true* or *false*.

- $P(CWE285 = T) = \sum_{CWE16} P(CWE285 = T\ |CWE16)P(CWE16) = 0.15 \times 0.24 + 0.02 \times 0.76 = 0.05$

Secondly, CWE287 is dependent on CWE89 according to the attack graph. NPT of the vulnerability CWE287 is calculated using the Equation 4. The probability of CWE287 is *true* given CWE89 is *true* or *false*.

- $P(CWE287 = T) = \sum_{CWE89} P(CWE287 = T|CWE89)P(CWE89) = 0.09 \times 0.1 + 0.04 \times 0.9 = 0.05$

The value 0.05 as the result of both equations indicates that there is a 5% chance that CWE285 is *true* and there is a 5% chance that CWE287 in *true*.

The values of NPTs for CWE285 and CWE287 presented in the table take into account that if vulnerability CWE16 or vulnerability CWE89 have been exploited, then the dependent probabilities of CWE285 or CWE287 need to be revised. The belief about the probability of CWE285 or CWE287 could be revised using the Bayes' theorem in Equation 3.

The same applies, if it is observed that the vulnerability CWE285 or CWE287 has been exploited, then the belief about the probability of CWE16 or CWE89 could be revised using the Bayes' theorem. If it is known that the vulnerability CWE285 is *true*, it potentially leads to an increased probability that CWE16 is *true*. The posterior probability of CWE16 can be calculated with Equation 3. As the result of the calculation is not used in the upcoming analysis, this information has only been presented to illustrate the potential use of Bayes' theorem. The same analysis can be conducted if the vulnerability CWE287 is observed to be exploited. If relevant data is gathered, the probabilities can be updated according to the same theorem. The calculated probabilities can be used to reason about the risk. These six NPTs are used to form the result of the BNBAG analysis in the next chapter.

## 5.4 Reasoning and Calculation in Outsourcing System Using BNBAG

The probabilities of the vulnerabilities found in the system have been calculated in the previous section. An incident can potentially occur if at least one vulnerability is successfully exploited. If two or more vulnerabilities are exploited, the probability of an incident is the sum of the probabilities of vulnerabilities described in Equation 9. To calculate the probability of an incident, the NPTs of the vulnerabilities have to be used.

There are 6 vulnerabilities illustrated in the attack graph. This means that there are 64 combinations of the vulnerabilities that could potentially lead to a successful incident. To give an overview of the results, two probabilities have been calculated. The probability of an incident is the probability that at least one vulnerability becomes exploited. The first probability of an incident has been calculated using vulnerabilities as independent events. The second probability of an incident considers also the conditioned probabilities in the calculation.

1. $P(incident) = 1 - \prod P(vulnerabilities = F) = 0.54$
2. $P(incident) = 1 - \prod P(vulnerabilities = F) = 0.56$

The results are different from each other. If no dependencies have been considered, the probability of an incident is 0.54. If the dependencies between vulnerabilities have been considered, the probability of an incident is 0.56.

The vulnerabilities can be categorized according to their severity which is defined as the probability of the vulnerability existing in the system and the likelihood of its exploit. The following list represents the vulnerabilities according to their severity:

| | | |
|---|---|---|
| 1. | CWE16 | Security misconfiguration |
| 2. | CWE79 | Cross-site scripting |
| 3. | CWE89 | SQL injection |
| 4. | CWE319 | Cleartext transmission of sensitive information |
| 5. | CWE287 | Improper authentication |
| 6. | CWE285 | Improper authorization |
| 7. | CWE937 | Using component with known vulnerabilities |
| 8. | CWE778 | Insufficient security logging |

In conclusion, BNBAG method can be used to evaluate information security risks. An illustration of the process has been shown in the chapter.

## 5.5 Chapter Summary

An overview of likelihood estimation within information security risk assessment using BNBAG method has been given in this chapter. Firstly, the relevant vulnerabilities of the implementation phase of the outsourcing system have been identified. OWASP Top 10 vulnerability taxonomy has been applied in the analysis, as it has been used in the financial institution before. The dependencies between the vulnerabilities have been defined and illustrated in the attack graph. To calculate the node probability tables of the assessed vulnerabilities, OWASP Top 10 data from the official repository has been used. The description of the data is given in Appendix I and Appendix II. The result of the risk likelihood estimation using BNBAG has been calculated, indicating the probability of an incident in the system. Overall, an illustration of how to consider correlated vulnerabilities within information security risk assessment using BNBAG method has been included in this chapter.

# 6 Discussion

To answer the research question, firstly, a security risk management method and a probabilistic risk assessment method have been compared, mapping their similarities and differences of domain models, metrics and processes. Thereafter, the methods have been applied to assess risks in the implementation phase of outsourcing to understand their similarities and differences in practice. In this chapter, a comparison of the results and observations of the two methods are presented. Description of how to combine the methods is shown. Feedback and validation of the results of the risk assessments and the list of steps to combine are given by the experts from the financial institution. Additionally, the limitations of the current study are added.

## 6.1 Comparison of ISSRM and BNBAG Methods

There are aspects to consider while choosing a risk assessment method. The decision needs to be made following the criteria that an organization has determined. In the following paragraphs, a comparison of ISSRM method and BNBAG method is presented, based on the case study experience of the author. The following characteristics of methods are considered: comprehensiveness, input, metrics, result, data related aspects, and resource related aspects.

The *comprehensiveness* of ISSRM method and BNBAG method is different. ISSRM method offers the user the opportunity to assess information security risk considering a number of domains, incl. assets, threats, vulnerabilities, impact, risk treatment and control. BNBAG method focuses only on the vulnerabilities of the information system. It is possible to combine ISSRM method and BNBAG method. This combination of methods can improve the overall assessment of information security risks. The list of recommendations, how to do it, has been presented in Section 6.2.

The two methods use different *input* to conduct the analysis. ISSRM method is based on the subjective input from the experts, who help to define relevant assets, threats and vulnerabilities. BNBAG method uses probabilistic values, which can be collected from the experts or calculated form data. The input values are needed to evaluate or calculate the probability of the vulnerability being present in the system and its likelihood of exploit.

ISSRM method proposes a number of *metrics* to calculate the results. In five cases, the metrics take the value of a number, based on expert opinion. The potentiality metric and risk level has been calculated from the input data of the expert. The logic behind the calculation of metrics within ISSRM method is not always transparent. Nonetheless, the calculations are easy given the input and using the proposed equations. BNBAG method uses Bayesian probability equations to calculate the needed probabilities. Calculation of explicit probabilities requires high maturity of understanding of business processes, vulnerabilities and systems from an organization. Therefore, its application makes sense only in case of sufficient maturity level within the organization. BNBAG application also requires basic quantitative skills from risk analysts, who are implementing the method.

ISSRM method defines risk as a threat exploiting a vulnerability leading to a potential impact for the organization. BNBAG addresses probability of one or many vulnerabilities being exploited leading to one or more incidents, which provides a part of overall risk assessment. Due to the different *scope*, the *results* need to be interpreted differently. ISSRM method uses scenarios to model risks. It represents a list of prioritized risk scenarios as the result. BNBAG method enables dependencies between vulnerabilities to be taken into account during risk estimation. It represents the probability of an incident using independent vulnerabilities or dependent vulnerabilities. Also, it results as a list of vulnerabilities according to their severity considering their prevalence in the system and likelihood of exploit.

There are some data-related aspects to consider while comparing the methods. Firstly, *data accessibility* is different between the two methods. ISSRM method uses expert opinions as input to the analysis. Although the success of the assessment depends on good communication between the experts, it is a rather simple technique. BNBAG method uses either expert opinions or gathered data as input to the analysis. Defining the relevant data and gathering it is more challenging than using expert opinion.

Secondly, *data reliability* aspect is different between the two methods. Theoretically, the most reliable source is measured data, followed by data, which is calculated, and the least reliable is data which is based on qualitative estimates. This means that if data in BNBAG analysis is measured, then the results will be more reliable than the results of ISSRM, which are based on qualitatively estimated data.

There are resource-related aspects to consider while comparing the methods. There are differences in the *scope of preliminary work* needed to start with risk assessment. ISSRM uses experts as their input for the analysis, therefore no preliminary work is needed. Experts gather their knowledge during everyday life and no extra work is needed before starting the risk assessment process. If quantitative data is used in BNBAG analysis, then the data requirements have to be determined, a script for processing it has to be developed and quality checks have to be done. Preliminary work is needed to start assessing risks with BNBAG.

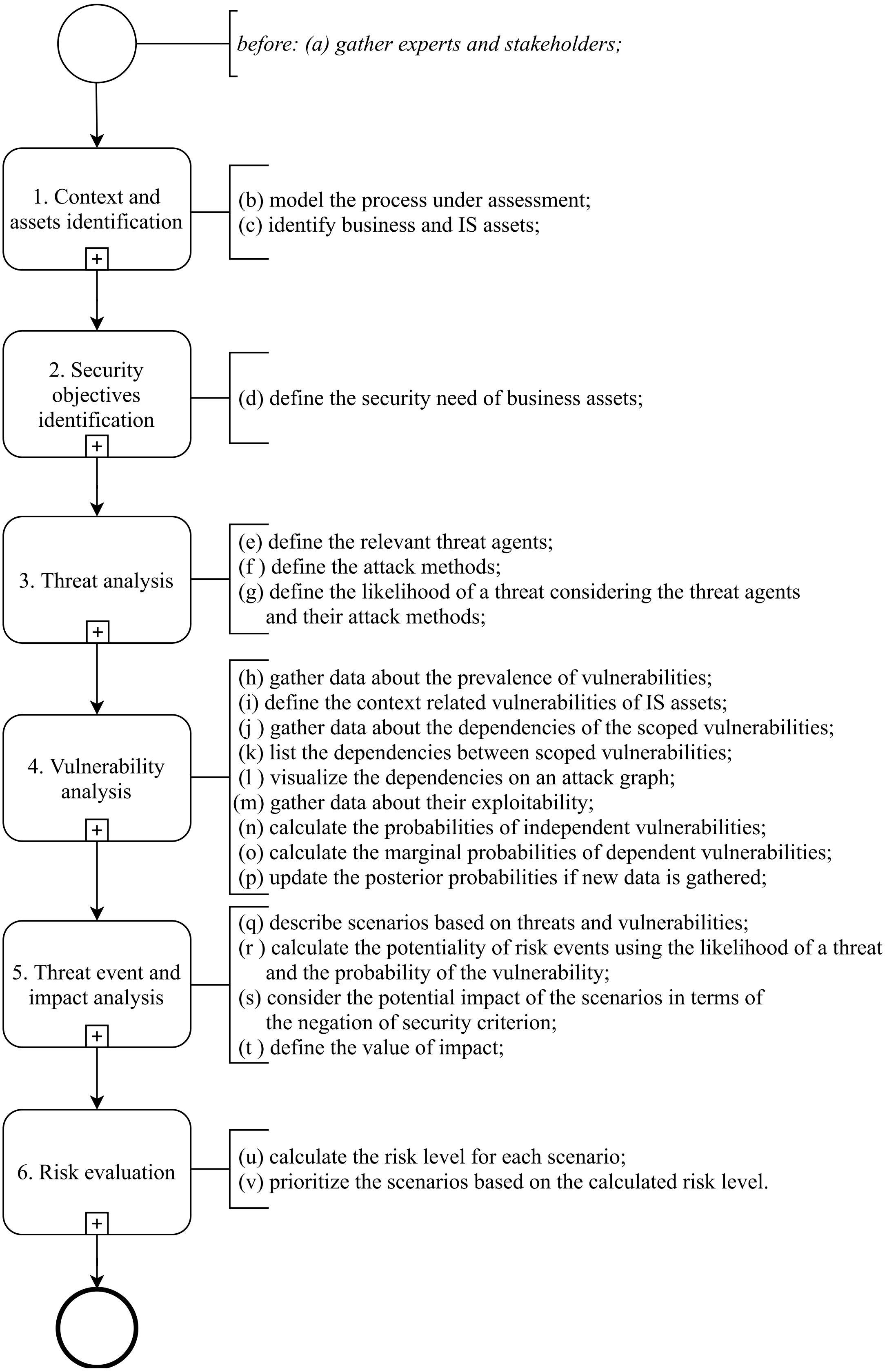
The other resource-related aspect is the *need for experts,* who have knowledge about the subject. Successful risk assessment relies on their input and effort to conduct it. The cost of hiring experts or using consulting companies can be used to measure the cost. The expert input is needed every time when risks are assessed with ISSRM method. BNBAG method also requires experts, who have expertise in both information security and data analysis and statistics. It could be possible to automate parts of the assessment process if the data analysis software is capable of incorporating new data and developing the structure of the network based on gathered data. Also, if the algorithms are capable of learning information from data, then it would also enable process automation.

These are a selection of criteria that an organization should consider. An organization has to define its requirements that have to be satisfied with the risk assessment method. The requirements depend on the regulatory landscape, the maturity level of the organization, budgeting decisions, and many other factors.

## 6.2 Towards Combination of Methods

To answer the research question, how to combine a security risk management method and a probabilistic risk assessment method, the following process has been proposed. The *comprehensiveness* of ISSRM method and BNBAG method is different. ISSRM method incorporates a number of domains that can be considered in risk assessment. However, the method uses estimated data as input which makes the results less reliable. BNBAG method is a limited method, focusing only on the assessment of vulnerabilities. Yet, measured data can be used an input to the analysis, which makes the results more reliable. It has been suggested by the author to combine ISSRM method and BNBAG method to provide enhancements to assessing information security risks.

In the following Figure 13., the process of assessing information security risk using the combination of a security risk management method and a probabilistic risk assessment method has been illustrated.



before: (a) gather experts and stakeholders;
1. Context and assets identification
(b) model the process under assessment;
(c) identify business and IS assets;
2. Security objectives identification
(d) define the security need of business assets;
3. Threat analysis
(e) define the relevant threat agents;
(f ) define the attack methods;
(g) define the likelihood of a threat considering the threat agents and their attack methods;
4. Vulnerability analysis
(h) gather data about the prevalence of vulnerabilities;
(i) define the context related vulnerabilities of IS assets;
(j ) gather data about the dependencies of the scoped vulnerabilities;
(k) list the dependencies between scoped vulnerabilities;
(l ) visualize the dependencies on an attack graph;
(m) gather data about their exploitability;
(n) calculate the probabilities of independent vulnerabilities;
(o) calculate the marginal probabilities of dependent vulnerabilities;
(p) update the posterior probabilities if new data is gathered;
5. Threat event and impact analysis
(q) describe scenarios based on threats and vulnerabilities;
(r ) calculate the potentiality of risk events using the likelihood of a threat and the probability of the vulnerability;
(s) consider the potential impact of the scenarios in terms of the negation of security criterion;
(t ) define the value of impact;
6. Risk evaluation
(u) calculate the risk level for each scenario;
(v) prioritize the scenarios based on the calculated risk level.

Figure 13. Process of combining a security risk management method and a probabilistic risk assessment method

To start with, (a) experts and relevant stakeholders have to be engaged into the risk assessment process. Firstly, their input is needed to (b) model the process under assessment. For example, BPMN language can be used to visualize the process. As a result of the process modelling, (c) business assets and their supporting IS assets are identified.

Secondly, the (d) security need of the business assets have to be defined. Information security need is usually determined using confidentiality, integrity, or availability as the objectives. However, other objectives that characterize the process can be used, e.g. non-repudiation, accountability, authenticity.

Thirdly, threats have to be analysed. The relevant (e) threat agents and their (f) attack methods have to be defined. It is possible to use threat landscape reports, e.g. ENISA Threat Landscape Report [38] or Europol Report [39], which give an overview of the most popular threat agents and attack methods. Also, there are threat taxonomies available for use, e.g. MITRE's ATT&CK taxonomy [22], Threat Agent Library by Intel Corporation [23], ENISA taxonomy [24]. The (g) likelihood of a threat for the organization has to be measured. It is difficult to measure the likelihood of a threat. Expert input is needed to define the value between zero and one, where zero indicates that there is no threat at all, and one indicates that there is a definite threat for the organization. Such evaluation is needed in further analysis.

The next phase is about vulnerability analysis. There are vulnerability taxonomies, e.g. OWASP Top 10 [27], Seven Pernicious Kingdoms [43], Common Vulnerabilities and Exposures [25], and it is possible to use a probabilistic assessment method. The key question is whether the organization is capable of gathering the relevant data. (h) Data about the prevalence of the vulnerabilities have to be gathered. Vulnerability scanning tools, e.g. Nessus tools [44], OpenVAS [45], can be used to gather information. The (i) context related vulnerabilities and their prevalence have to be defined. Prevalence is the quantity of the certain vulnerability found in tested network and applications. (j) Data about the dependencies between the vulnerabilities have to be found. It is possible to use expert knowledge or advanced algorithms, e.g. constraint-based algorithms based on inductive causation [46], or score-based algorithms [47], to find the dependencies. The potential (k) dependencies between vulnerabilities have to be defined and (l) visualized on an attack graph. It is possible to use RStudio and write an R script to plot the attack graph based on the defined vulnerabilities and their dependencies between each other. (m) Data about the likelihood of exploit of each vulnerability has to be gathered. It is possible to use expert knowledge to gather such data. The (n) probability of a vulnerability is the probability of prevalence multiplied with the likelihood of exploit. The (o) probabilities of dependent vulnerabilities are the marginal probabilities of the vulnerabilities. It is possible to (p) update the posterior probabilities using the Bayes' theorem if new data is gathered. The values are between zero and one.

The following phase is about threat events which lead to an impact. (q) Scenario-based threat modelling can be used. The scenarios should consider a potential threat agent with an attack method to exploit a vulnerability. The (r) potentiality of a threat event is the product of the likelihood of the threat and the probability of the vulnerability. (s) Impact of the threat events has to be considered in terms of confidentiality, integrity, and availability of the business asset. (t) Value of impact has to be defined.

Risk evaluation is the last phase of risk assessment. The (u) risk level value is the product of the potentiality of a threat event and the impact value. The (v) scenarios have to be prioritized according to the calculated risk level. This means that the risk scenario which received the highest risk values becomes the first one on the list. The risk scenario which received the lowest risk level value becomes the last one on the list.

## 6.3 Feedback from the Financial Institution

This section discusses the feedback provided by the financial institution for the thesis. It gives a description of the procedure and an overview of the participated experts. The feedback is essential to validate the correctness and completeness of the thesis and discuss its usefulness for the industry.

**Description of the procedure**

The feedback was asked from the selection of financial institution employees. The decision of whom to ask for their input was based on their expertise in risk assessment or outsourcing. Each participant holds a non-disclosure agreement with the financial institution. The participants were invited via e-mail to participate in the feedback meeting of the thesis. Beforehand, an overview of the research problem and questions, scope, methodology and contribution were provided for them. The invited experts decided whether to participate in the meeting or not. Overall, seven experts joined the meeting via Skype and four experts were present in the meeting room. The following areas of experts were present in the meeting: operational risk, information security, third-party outsourcing, and procurement.

The author of the research gave a presentation about the thesis for the audience. The relevance of the topic and the research problem were explained. The research questions, which have been proposed in the thesis, were discussed. An overview of the included methods was given, emphasizing the differences between the processes, the used metrics and the results. Also, the outsourcing process which is the context of the risk assessment was introduced. The outsourcing process description had been validated before by the expert of outsourcing in the financial institution. The results of the ISSRM method and BNBAG method were represented, explained and compared. Finally, the recommended steps for how two combine the methods were described. The feedback was given after the end of the presentation and additional comments about the correctness and completeness were sent via email. The citations in the following paragraphs have been taken from the written emails forwarded to the author from the experts.

**Validation and discussion**

The participants were asked about the correctness and completeness of the defined problem statement, procedure, and results. The problem statement was evaluated to be correctly defined reflecting the challenges that the organization faces in their everyday operations. It was emphasized that "*organizations struggle with information security risk assessment due to its interdisciplinary nature as well as a vague understanding of the specific risks on the executive management level".* Qualitative information risk assessment methods are industry best practice. However, "*qualitative methods are inefficient in providing a versatile view*". Some other areas assess risks using quantitative methods which are reliable as they are based on measured data. Therefore, "*all efforts towards quantitative risk measurement and assessment methodologies are essential and highly appreciated*". However, the comments suggested that the problem statement was not complete as "*outsourcing would have had to be considered in the context of a selected critical process, not the risks associated with outsourcing process as such*".

The overall procedure of the thesis was also discussed with the meeting participants. It was validated to be complete, understandable and easy to follow. The research paper "*follows a coherent track from containing a specific example of application to how qualitative and quantitative assessment can be recorded and used for it*". Feedback about the conclusions and case representation was also given indicating its admissibility in the context of the financial institution. However, there was a comment about the correctness of the research procedure as the problem statement has been proposed on a high-level while the methods consider a small step in the outsourcing process and make risk estimation at a very detailed level. Yet, it was understood that "*the full framework for risk aggregation might have been too high ambition*".

The results of the research were also reviewed by experts. The results were considered to be correct as of the data, its interpretation and calculations led to clear and understandable results. It was implied that the results were not complete as "*the results of the risk assessment methods are only illustrative examples of the usage of methods". The results of the risk assessments do not explicitly describe the situation in the financial institution because industry-specific data has not been used in the analysis. Yet, "*the value of such scope is setting a more general basis to support the choice and design of risk assessment methodologies, as the principles can be embedded in various process models*".

Some other discussion points emerged from the meeting session. Feedback about the importance of the partnership between academia and industry in the field of information security was pointed out. The financial institution is known for having co-supervised students in the areas of economics and finances. Yet, information security-based research done as a year-long cooperation is new for the organization. It was highlighted that such "*partnership between academia and industry is inevitable for moving forward with information security risk assessment methods"*. The experts acknowledge that "*the area is still very much in development and out-of-the box solutions have not matured*".

The meeting also included a discussion about the challenges that an organization should first overcome to use a probabilistic risk assessment method. It was noted that the research paper highlights the *"need of sufficient maturity to assess risks quantitatively"*. The prerequisites for assessing risks quantitatively or using a combination of a qualitative and quantitative method have to be met. The needed data and its gathering process have to be defined. Also, "*understanding of risks and ownership of data and processes before moving towards advanced quantitative methods is needed".*

The topic of outsourcing and its related information security risks was also discussed. The importance of understanding the risks related to outsourcing was emphasized. It was remarked that organizations still face the *challenges of coordination, structured data, and optimal risk management processes*. This indicates that certain issues have to be settled before moving forward with the applications of quantitative methods.

Lastly, the experts suggested further doing the cost analysis, proof-of-concept on aggregated risk levels, but also evidence of competence and data quality to enable the combined method or alternative methods with similar characteristics.

## 6.4 Limitations of the Study

There are certain limitations to the study. The missing part of the research is the risk assessment of *third-party access to the systems* of the financial institutions and the *integration between the systems* of the service provider and the financial institution. Threat could have modelled by building the *attack vectors from the service provider to the financial institution*. Such analysis would have required detailed knowledge about the vulnerabilities of the information system assets of the service providers and the volume and level of detail of such analysis would have been out of the scope of this thesis.

The research considers outsourcing as requesting services and solutions from external parties. However, the financial institution uses *internal outsourcing*, i.e. requiring services or solutions produced by another department within the bank, *as another option* which has not been covered in the thesis. Risk could potentially have different characteristics whether the services have been provided by external parties or internal employees. Outsourcing to *cloud service providers* is also not considered in the study, although its importance has increased in the last years. The risk scenarios and results could have been different if cloud service providers would have been included in the analysis.

The research paper considers the adversarial threats for the organization. However, *accidental threats* that are caused by the organization's own employees have not been analysed. Humans can easily make mistakes due to their careless attitude, lack of awareness about the issues, or any other personal characteristic. Human aspects of information security risk are important to be considered while evaluating the risks.

Data-related limitations concern the *lack of data*, *use of available data* in the analysis, and the *incorporated expert judgement data*. The analysis in this thesis is not performed on specific data of a single financial institution to allow to make more generic conclusions. Furthermore, the results are not thoroughly financial sector specific, as e.g. other vital service providers face very similar challenges to financial sector institutions in terms of assessing information security risk. This is both a strength of the work, allowing to draw conclusions, which can be used in many different frameworks, but also a weakness, as the author cannot conclude step-by-step proof-of-concept based on a specific example. These limitations should be taken into consideration to improve the research in the future.

## 6.5 Chapter Summary

This chapter summarizes the discussion about the results of the thesis. Firstly, a comparison has been included according to the observations made during the risk assessment processes. The two methods have been compared in terms of their *comprehensiveness*, *input data, metrics and results*, *other data-related aspects* and *resource-related aspects*. Secondly, an overview of the recommended steps on how to combine the methods has been presented in Figure 13. The description of the steps has been included. Thirdly, a description about the feedback from the financial institution has been added, covering the relevance of the topic for the sector, feedback on the structure and content of the thesis, and future research suggestions. Finally, the limitations of the scope of current research have been presented.

# 7 Conclusion

The opportunities that the use of technology and information provides, ensure that private individuals, fields of industries, and governments will continue to use them extensively and find new advanced ways to integrate them more and more into their everyday operations. If there are opportunities, there are also risks. Today, the financial institution uses security risk management methods that are qualitative to assess their information security risk. Another option would be to assess security risk using a probabilistic method. ISSRM method has been chosen to represent a risk management method while BNBAG method serves as a probabilistic risk assessment method. The two methods have been applied in a case study to grasp their similarities and difference in practice. Outsourcing has been chosen as the context to implement the two methods. Outsourcing is one of the top challenges in the financial sector. The results of the two assessments have been presented. Applying the methods to assess the information security risk of a real-life process has given the author of the thesis an understanding that enhancements in the field are needed. A suggestion on how to combine a security risk management method and a probabilistic method has been given. The answers to the research questions have been provided in the following paragraphs.

*Research question 1: What are the assets that need protection?*

The relevant assets that need protection in the context of outsourcing in the financial institution have been identified. The process of outsourcing has been described and modelled to determine the assets. An outsourcing handbook issued by the financial institution has been used as the basis for modelling the process. The overall outsourcing process consists of five stages represented in Figure 5. To narrow the scope, only the implementation phase has been used in risk assessment. The process of implementation includes *Outsourcing agreement signing*, *Outsourcing agreement storing*, *FSA notification* and *Testing and implementation*. The BPMN modelling language has been used to identify the assets that need protection in the implementation phase of outsourcing. The process models illustrate business and information system assets that support business assets. The identified assets have been discussed in Section 3.5. The assets that need protection are both the business assets as well as the system assets. The business assets need protection as the adversary's motivation can be either to disclose, modify, or disrupt the business asset. The information system assets also need protection as they support business assets. The vulnerabilities which are the characteristics of the information system assets can be exploited by the adversary; thus, additional protection of the information system assets is needed. It has been illustrated in the thesis, how security risk management method is based on asset-related concepts, i.e. the main focus is on identifying and protecting the assets. Assets need to be identified to understand the related vulnerabilities, which could be exploited by a threat leading to an impact for the organization.

*Research question 2: What is the estimated information security risk?*

Information security risk has been assessed with two methods. ISSRM method describes the information security risk as to the combination of a threat exploiting one or more vulnerabilities, leading to an impact for the organization. Threat agents and their potential attack methods have been described using ENISA taxonomy introduced in Section 2.1. The threats are relevant to the implementation phase of the outsourcing process due to the existing vulnerabilities in the information system assets. The vulnerabilities have been assessed using the OWASP Top 10 taxonomy introduced in Section 2.1. Firstly, risk scenarios have been developed where a threat exploits a vulnerability of an information system asset which leads to an impact that negates the security criterion. The metrics that are proposed by the ISSRM method have been calculated to achieve the result presented as a list of risk levels. The security risk assessed with ISSRM method has been presented in Chapter 4. Secondly, BNBAG method has been used to model dependencies between vulnerabilities. The main focus has been on identifying the relevant vulnerabilities and the directed dependencies between them. Again, the vulnerabilities have been assessed using the OWASP Top 10 taxonomy. An attack graph made of the vulnerability nodes has been created to illustrate the dependencies between vulnerabilities. The node probability tables for each vulnerability has been calculated. The result is the probability of an incident. The security risk assessed with BNBAG method has been presented in Chapter 5.

*Research question 3: What is the comparison of the chosen risk assessment methods?*

The comparison between the security risk management method and the probabilistic risk assessment method has been described. The comparison has been made based on the subjective observations made during the risk assessment processes. Firstly, the two methods have been compared in terms of their *comprehensiveness*. ISSRM method offers a coherent overview of a risk considering asset-related concepts and risk-related concepts as part of the assessment process. BNBAG method focuses only on the assessment of vulnerabilities to calculate the probability of an incident. Secondly, while ISSRM method uses qualitative data as *input* to the analysis, it is possible to use measured data in BNBAG analysis. The *calculation of the result* is different; hence, the *result* of the methods is also different. Also, the comparison is made in terms of data-related aspects, including *data accessibility* and *data reliability*. Additionally, the methods have been compared in terms of resource-related aspects, such as the *scope of preliminary work* and the *need for experts*. The comparison between the processes, models, and metrics of the two methods has been presented in Section 2.4. The comparison based on the observations made during the risk assessment processes has been presented in Section 6.1.

*Research question 4: How can security risk management method and probabilistic risk assessment method be used together?*

It has been suggested by the author of the thesis to combine the security risk management method and the probabilistic risk assessment method to improve the results of the risk assessment. It has been recommended to combine the methods using the following stages: identification of the assets and the security objectives based on ISSRM method, analysis of threats according to ISSRM method, modelling of vulnerabilities based on BNBAG, description of threat events and the potential impact using ISSRM. The steps have been described in Section 6.2. The combined method offers an opportunity to use both expert knowledge and quantitative data in the analysis, resulting in a more reliable information security risk assessment for the organization.

There are future research suggestions to be considered. Information security risk assessment methods can be improved to start making budgeting decisions based on relevant data, calculations, and reasoning. Although it depends on the maturity level of the organization, Bayesian network modelling could be beneficial if it is based on accurate data and validated graph visualization. There is further research needed to define the relevant data, the source from which the data should be gathered, and the requirements that the data needs to satisfy. Also, there is research needed to determine the possibilities of how to form the structure of the graph that would describe the gathered data to assess risks. Although there are algorithms available for use, the most suitable one should be determined. Also, additional research could be made to define Bayesian network-based attack graphs improvement options. It could be possible to include decision and utility nodes in the Bayesian network or cost-benefit analysis. These are the future research suggestions for the financial institution to conduct.

## References

[1] International Telecommunication Union, “Measuring the Information Society Report,” 2018. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR2018-ES-PDF-E.pdf. [Accessed 3 January 2019].

[2] International Telecommunication Union and World Telecommunication, “Individuals using the Internet (% of population),” International Telecommunication Union, 2018. [Online]. Available: https://data.worldbank.org/indicator/IT.NET.USER.ZS. [Accessed 3 January 2019].

[3] D. Reinsel, J. Gantz and J. Rydning, “Data Age 2025: The Evolution of Data to Life-Critical,” International Data Corporation, sponsored by Seagate, Framingham, Massachusetts, 2017.

[4] A. Hunt, E. Thrower, M. Yeomans and B. Heynderickx, “Quantitative Techniques in Information Risk Analysis,” Information Security Forum, 2018.

[5] S. L. Savage, The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty, Hoboken, New Jersey: John Wiley & Sons, Inc., 2009, p. 155.

[6] Institute of Risk Management, “A Risk Practitioners Guide to ISO 31000: 2018,” Institute of Risk Management, London, 2018.

[7] British Standards Institution and ISO/IEC, “Information technology — Security techniques — Information security risk management,” BSI, London, 2008.

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

[9] N. Fenton and M. Neil, Risk Assessment and Decision Analysis with Bayesian Networks, Boca Raton: Taylor & Francis Group, 2013.

[10] L. Munoz-Gonzalez and E. C. Lupu, “Bayesian Attack Graphs for Security Risk Assessment,” in *IST-153 Workshop on Cyber Resilience*, Munich, 2017.

[11] Basel Committee on Banking Supervision, “The Joint Forum: Outsourcing in Financial Services,” February 2005. [Online]. Available: https://www.bis.org/publ/joint12.pdf. [Accessed 9 February 2019].

[12] European Banking Authority, “Risk Assessment of the European Banking System,” December 2018. [Online]. Available: https://eba.europa.eu/documents/10180/2518651/Risk_Assessment_Report_December_2018.pdf. [Accessed 11 May 2019].

[13] L. Õunapuu, Kvalitatiivne ja Kvantitatiivne Uurimisviis Sotsiaalteadustes, Tartu: Tartu Ülikool, 2014.

[14] A. Shameli-Sendi, R. Aghababaei-Barzegar and M. Cheriet, “Taxonomy of Information Security Risk Assessment (ISRA),” *Computers & Security,* vol. 57, pp. 14-30, 2016.

[15] ISO/IEC, “ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management,” 2018. [Online]. Available: https://www.iso.org/standard/75281.html. [Accessed 1 May 2019].

[16] ISO/IEC, “ISO/IEC 27000 family,” ISO, May 2019. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Accessed 1 May 2019].

[17] National Institute of Standards and Technology, “NIST Special Publication 800-30: Guide for Conducting Risk Assessment,” NIST, Gaithersburg, 2012.

[18] FAIR Institute, “Measuring and Managing Information Risk: a FAIR Approach,” [Online]. Available: https://www.fairinstitute.org/fair-book. [Accessed 1 May 2019].

[19] R. A. Caralli, J. F. Stevens, L. R. Young and W. E. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” Carnegie Mellon and Software Engineering Institute, 2007.

[20] COSO, “Enterprise Risk Management - Integrated Framework,” September 2004. [Online]. Available: https://www.coso.org/Pages/erm-integratedframework.aspx. [Accessed 1 May 2019].

[21] Financial Sector Advisory Center of World Bank Group, “Financial Sector's Cybersecurity: A Regulatory Digest,” October 2017. [Online]. Available: http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf. [Accessed 8 January 2019].

[22] MITRE Corporation, “MITRE ATTA&CK,” 2018. [Online]. Available: https://attack.mitre.org. [Accessed 6 April 2019].

[23] T. Casey, “White Paper: Threat Agent Library Helps Identify Information Security Risks,” September 2007. [Online]. Available: https://pdfs.semanticscholar.org/391e/70510353ba762fa1580a6d9c002eefd2d86b.pdf. [Accessed 6 April 2019].

[24] ENISA, “Threat Taxonomy,” September 2016. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view. [Accessed 19 April 2019].

[25] MITRE Corporation, “CVE Common Vulnerabilities and Exposures,” MITRE Corporation, 2019. [Online]. Available: https://cve.mitre.org. [Accessed 6 April 2019].

[26] National Institute of Standards and Technology, “National Vulnerability Database,” NIST, [Online]. Available: https://nvd.nist.gov. [Accessed 4 May 2019].

[27] OWASP Foundation, “OWASP Top 10,” 2017. [Online]. Available: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf. [Accessed 3 April 2019].

[28] D. W. Hubbard, How to Measure Anything: Finding the Value of "Intangibles" in Business, Hoboken, New Jersey: John Wiley & Sons, Inc., 2007.

[29] D. Kelly and C. Smith, Bayesian Inference for Probabilistic Risk Assessment: A Practitioner's Guidebook, London: Springer, 2011.

[30] M. Frigault, L. Wang, S. Jajodia and A. Singhal, “Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks,” in *Network Security Metrics*, Switzerland, Springer International Publishing AG, 2017, pp. 1-23.

[31] U. B. Kjærulff and A. L. Madsen, Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis, vol. II, New York: Springer, 2013.

[32] S. Cullen, P. Seddon and L. P. Willcocks, “Domberger's Theory of Contracting Applied to IT Outsourcing,” in *Information Systems and Outsourcing*, New York, Palgrave Macmillan, 2009, p. 130.

[33] R. Pompon, IT Security Risk Control Management: an Audit Preparation Plan, Settle: Apress, 2016, pp. 283-284, 287.

[34] Estonian Parliament, “Riigi Teataja: Emergency Act,” 1 July 2017. [Online]. Available: https://www.riigiteataja.ee/en/eli/525062018014/consolide. [Accessed 9 February 2019].

[35] D. Singh, “Outsourcing in Financial Services,” *Journal of Banking Regulation,* vol. VI, no. 3 , p. 202–204, 1 May 2005.

[36] European Parliament and European Council, “Directive 2014/65/EU "Markets in Financial Instruments Directive",” 15 May 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=ET. [Accessed 9 February 2019].

[37] European Parliament and European Council, “Directive 2015/2366/EU "Payment Service Directive 2",” 25 November 2015. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN. [Accessed 9 February 2019].

[38] ENISA, “Threat Landscape Report 2018,” January 2019. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018. [Accessed 26 March 2019].

[39] Europol, “Internet Organised Crime Threat Assessment (IOCTA) 2018,” 2018. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018. [Accessed 26 March 2019].

[40] OWASP Top 10 project, “Official OWASP Top 10 Repository,” 2017. [Online]. Available: https://github.com/OWASP/Top10/tree/master/2017/datacall/analysis. [Accessed 3 April 2019].

[41] MITRE Corporation, “CWE List Version 3.2,” MITRE Corporation, 11 December 2018. [Online]. Available: https://cwe.mitre.org/data/index.html. [Accessed 3 May 2019].

[42] MITRE Corporation, “CWE-287: Improper Authentication,” January 2019. [Online]. Available: https://cwe.mitre.org/data/definitions/287.html. [Accessed 20 April 2019].

[43] MITRE Corporation, “Seven Pernicious Kingdoms,” 3 January 2019. [Online]. Available: https://cwe.mitre.org/data/definitions/700.html. [Accessed 15 May 2019].

[44] Tenable Inc., “The Nessus Family,” 2019. [Online]. Available: https://www.tenable.com/products/nessus. [Accessed 15 May 2019].

[45] Offensive Security, “OpenVAS Vulnerability Scanning,” 2019. [Online]. Available: https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/. [Accessed 15 May 2019].

[46] J. Pearl and T. S. Verma, “A Theory of Inferred Causation,” 1991. [Online]. Available: https://ftp.cs.ucla.edu/pub/stat_ser/R156.pdf. [Accessed 15 May 2019].

[47] M. Scutari and J.-B. Denis, Bayesian Networks with Examples in R, London: CRC Press, 2015, pp. 106-107.

# Appendix

## I. Description of Data

| OWASP category | Vulnerability | ID | Sample size | Mean | Standard deviation | Likelihood of exploit |
|---|---|---|---|---|---|---|
| Injection | SQL Injection | CWE89 | 11929 | 458,81 | 976,54 | High |
| Broken authentication | Improper Authentication | CWE287 | 4258 | 163,77 | 486,42 | High |
| Sensitive data exposure | Cleartext Transmission of Sensitive Information | CWE319 | 5782 | 222,38 | 690,75 | High |
| XXE | XML External Entity Injection (XXE) | CWE611 | 9658 | 371,46 | 1035,29 | High |
| Broken access control | Improper Authorization | CWE285 | 2641 | 101,58 | 252,03 | High |
| Security misconfiguration | Security Misconfiguration | CWE16 | 28526 | 1097,15 | 3985,01 | High |
| Cross-site scripting | Cross-Site Scripting (XSS) | CWE79 | 28503 | 1096,27 | 2033,40 | High |
| Insecure deserialization | Deserialization of Untrusted Data | CWE502 | - | - | - | Medium |
| Using components with known vulnerabilities | Using Components with Known Vulnerabilities | CWE937 | 1624 | 62,46 | 183,56 | Medium |
| Insufficient logging and monitoring | Insufficient Security Logging | CWE778 | 446 | 17,15 | 71,79 | Medium |
| Number of tested applications | | | 120847 | | | |

Source: Compiled by the author (base on OWASP Top 10 data)
Note: the symbol “-“ indicates that there is no data about this vulnerability in database.

## II. Overview of Data

| Organization | Vulnerabilities | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | CWE 79 | CWE 16 | CWE 319 | CWE 285 | CWE 937 | CWE 89 | CWE 287 | CWE 778 | CWE 611 |
| O1 | 306 | 12 | 135 | 4 | 88 | 54 | 116 | 0 | 0 |
| O2 | 2019 | 4390 | 3452 | 68 | 889 | 522 | 216 | 0 | 693 |
| O3 | 3423 | 0 | 81 | 6 | 25 | 1111 | 0 | 0 | 102 |
| O4 | 635 | 355 | 67 | 246 | 36 | 147 | 246 | 0 | 101 |
| O5 | 7513 | 20059 | 0 | 3 | 0 | 3896 | 6 | 0 | 4641 |
| O6 | 6130 | 0 | 0 | 0 | 0 | 2238 | 21 | 0 | 2570 |
| O7 | 4501 | 0 | 0 | 0 | 0 | 2627 | 18 | 0 | 1303 |
| O8 | 336 | 205 | 63 | 57 | 0 | 47 | 289 | 0 | 3 |
| O9 | 356 | 356 | 114 | 24 | 356 | 27 | 21 | 0 | 30 |
| O10 | 200 | 14 | 149 | 7 | 55 | 9 | 124 | 0 | 0 |
| O11 | 1040 | 400 | 1020 | 1100 | 40 | 780 | 400 | 364 | 200 |
| O12 | 111 | 0 | 22 | 76 | 111 | 50 | 70 | 0 | 2 |
| O13 | 47 | 99 | 115 | 148 | 0 | 17 | 0 | 0 | 0 |
| O14 | 147 | 27 | 87 | 144 | 0 | 13 | 155 | 62 | 0 |
| O15 | 1626 | 2490 | 407 | 727 | 0 | 267 | 2490 | 7 | 10 |
| O16 | 5 | 3 | 2 | 1 | 0 | 3 | 1 | 0 | 0 |
| O17 | 2 | 5 | 6 | 3 | 0 | 0 | 3 | 8 | 0 |
| O18 | 1 | 7 | 3 | 0 | 7 | 0 | 2 | 0 | 0 |
| O19 | 40 | 46 | 46 | 8 | 8 | 8 | 46 | 0 | 3 |
| O20 | 25 | 31 | 6 | 6 | 5 | 8 | 22 | 0 | 0 |
| O22 | 6 | 4 | 6 | 2 | 1 | 4 | 2 | 0 | 0 |
| O23 | 9 | 6 | 0 | 9 | 0 | 10 | 6 | 0 | 0 |
| O24 | 22 | 14 | 0 | 0 | 0 | 90 | 1 | 0 | 0 |
| O25 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| O26 | 2 | 3 | 1 | 2 | 3 | 1 | 3 | 5 | 0 |

Source: OWASP Top 10 data [40]

## III. R Code for Creating an Attack Graph

```
# Vulnerability-based attack graph
library(ggdag)
dag_vulnerabilities_mt<-dagify(Incident~CWE89+CWE285+CWE319+CWE79,
                         Incident~CWE287+CWE16+CWE778+CWE937,
                         CWE285~CWE16,
                         CWE287~CWE89)

ggdag(dag_vulnerabilities_mt, node_size=20, text_size = 3, layout="circle")
```

## IV. License

**Non-exclusive licence to reproduce thesis and make thesis public**

I, Kärt Padur,

(*author's name*)

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

reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

Information Security Risk Assessment in the Context of Outsourcing in a Financial institution,

(*title of thesis*)

supervised by Raimundas Matulevičius, Ph.D, Liis Rebane, Ph.D, Toomas Vaks, MA.

(*supervisor's name*)

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

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

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

*Kärt Padur*

***20/05/2019***