

**UNIVERSITY OF TARTU**  
**FACULTY OF MATHEMATICS AND COMPUTER SCIENCE**  
**INSTITUTE OF COMPUTER SCIENCE**  
**Cybersecurity Curriculum**

**Anna Preobrazenskaja**  
**Development of Security Risk Measurement Model**  
**within Misuse Cases and BPMN**

Master's thesis (30 ECTS)

Supervisor: Raimundas Matulevičius

TARTU, 2014

# **Development of Security Risk Measurement Model within Misuse Cases and BPMN**

## ***Abstract:***

One of the most important tasks of any organization is to secure its assets. Since no system could be made completely secure, in order to prevent security flaws, companies apply controls to safeguard their assets from different threats. Therefore, risk analysis is an important step for the management of information systems security (ISS). Today various ISS risk analysis methods have been developed, but they mainly provide general guidelines to estimate the risk. The problem defined in the thesis is how to measure the risk illustrated with the help of a modeling languages. For that two modeling languages were chosen: misuse cases and BPMN.

This is a problem, because we can see from a practical experience that the same security events are happening periodically, but the security risks are not treated. This may occur either because people do not see the repeated exploitation of vulnerabilities, the risk level and losses are not measured, considering the problems of a less importance. Without knowing exactly how much damage the security event makes, the management is not able to decide whether the risk should be fixed or not. If a risk is measured and values are visible, it is easier to do a proper decision about the risk mitigation.

Our goal is to help understand the severity of the security risks by visualizing the metrics and calculations of a risk. For that in modeling languages a visualization of thread cases is needed. Then security cases need to be measured. Today there is no existing model that can visualize the measurement together with the case itself. The contribution of this thesis will be the development of measurement model within misuse case and BPMN diagrams.

These models will facilitate the evaluation of an overall risk, by dividing the risk into sub-components and individually measuring the asset value, potentiality of thread, level of vulnerability. It will also give information about cost and benefit of implementation of countermeasures. This means that the metrics and the severity of a risk will be visible straight away. This will help the security specialist to make a decision whether the investment into a particular security flaw is reasonable or not. It should give a clear picture of the company's losses from exploitation of risk and will make it easier to understand whether it is a substantial loss or not.

Two models will be developed using both theoretical and empirical data. Existing assessment approaches and standards together with different modeling languages will be studied. At the same moment the cases from the working organization will be taken. Two models will be developed and applied to investigate the visibility of metrics proposed.

The developed security risk measurement models will give a solution how to calculate the risks taken from a real world example using misuse cases and BPMN. During validation we have tested our two models, which of them gives better visibility of the metrics introduced.

## **Keywords:**

Measurement model, evaluation model, assessment, modeling language, security risk, misuse case, risk management

# **Turvalisuse riskide mõõtmise mudeli arendamine väärkasutamise juhtumite (misuse cases) ja äriprotsesside modelleerimiskeele (BPMN) piirides**

## **Lühikokkuvõte:**

Iga organisatsiooni kõige tähtsam ülesanne on oma vara kaitsta. Kuna mitte ühtegi süsteemi ei ole võimalik täielikult turvaliseks teha, seega rakendavad ettevõtted erinevaid kontrole, et oma vara erinevate ohtude eest kaitsta. Riskianalüüs on üks oluline samm infosüsteemide (IS) turvalisuse tagamises ja tänaseks on välja töötatud erinevaid IS-de riskianalüüsi meetodeid, kuid need osutavad peamiselt üldisi suunised riskide hindamiseks. See dokument, aga käsitleb probleemi kuidas mõõta riski illustreerituna modelleerimiskeelte abist. Selleks on valitud kaks modelleerimise keelt: väärkasutamise juhtumid (Misuse Case) ja äriprotsesside modelleerimiskeel (BPMN).

Praktilisest kogemustest on näha, et samad turvaaukudega seotud sündmused toimuvad perioodiliselt ning nende järel turvalisusega seotud riske ei maandata. Seda sellepärast, et ei ole näha turvaaukude korduvat kasutamist või riskide erinevaid tasemeid ja kaotused ei ole mõõdetud, mistõttu arvestatakse, et turvaaukudega kaasnevad probleemid on vähem tähtsad. Teadmata, kui palju kahju üks turvalisusega seotud sündmus teeb, ei saa juhtorgan otsustada, kas tegeleda riski maandamisega või mitte. Kui riskid oleksid mõõdetud ja nende väärtused oleksid nähtavad, oleks lihtsam teha õigeid otsuseid riskide maandamiseks.

Selle töö eesmärk on aidata organisatsiooni juhtidel aru saada kui tõsised on turvalisusega seotud riskid, selleks visualiseerides meetrikaid ja tuues välja riskide kalkulatsioonid. Et seda teha ka modelleerimiskeeltes, tuleb selleks visualiseerida riskidega seotud juhtumeid. Alles seejärel on võimalik mõõta turvalisusega seotud juhtumite tõsisust. Selle töö kirjutamise hetkel ei eksisteeri ühtegi mudelit mis suudaks visualiseerida mõõtmist koos juhtumi endaga. Selle töö tulemusena arendatakse mõõtmismudel väärkasutamise juhtumite ja äriprotsesside modelleerimiskeele diagrammide piirides.

Need mudelid hõlbustavad üldise riski hindamist jagades riski alam-osadeks ja mõõdavad eraldi vara väärtust, ohu potentsiaalsust ja haavatavust. Samuti annavad need teavet riskide kulukuse kohta ja toovad välja vastumeetmete rakendamise kasulikkuse. See tähendab, et riski meetrika ja tõsisus on koheselt nähtav. See aitab turvalisuse spetsialistil teha otsuseid, kas mõne konkreetse turvariski maandamiseks investeerimine on mõistlik või mitte. See peaks andma ka selge pildi ettevõtte kahjumist, kui riske kasutatakse ära ja aitab mõista, kas see on märkimisväärne kaotus või mitte.

Kahe mudeli välja töötamiseks kasutades nii teoreetilisi kui ka empiirilisi andmeid, seega turvalisusega seotud riskide mõõtmise mudelid annavad lahenduse probleemile, kuidas arvutada riske mis on võetud pärismaailmast, kasutades selleks väärkasutamise juhtumeid ja äriprotsesside modelleerimiskeelt. Lisaks uuritakse olemasolevaid hindamise meetodeid ja standardeid koos erinevate modelleerimiskeeltega, ning töös kasutakse näiteid ühest töötavast organisatsioonist. Pärast mudelite välja töötamist need ka rakendatakse, et uurida väljapakutud meetrikate nähtavust. Valideerimise ajal võrreldakse kahte mudelit selgitamiseks välja milline nendest annab parema ülevaate juurutatud meetrikatest.

## **Võtmesõnad:**

Mõõtmise mudel, hindamise mudel, hindamine, modelleerimise keel, turvarisk, väärkasutamise juhtumid, riskijuhtimine, äriprotsesside modelleerimiskeel(BPMN), meetrika

## **Table of Contents**

Abstract: .....	2
Lühikokkuvõte: .....	3
Table of Contents .....	4
List of Figures .....	5
List of Tables.....	6
CHAPTER 1. Introduction .....	8
CHAPTER 2. Approaches for Security Risk Management .....	10
2.1 Introduction to security risk management .....	10
2.2 Standards .....	10
2.3 Security risk management methodologies.....	11
2.4 ISSRM domain model .....	12
2.4.1 Asset-related concepts.....	12
2.4.2 Risk-related concepts .....	13
2.4.3 Risk-treatment related concepts .....	13
2.4.4 ISSRM metrics .....	13
2.6 Summary .....	15
CHAPTER 3. Security Risk-Oriented Modeling .....	16
3.1 Security risk description.....	16
3.2 Misuse cases .....	17
3.2.1 Alignment of misuse cases to ISSRM Domain Model .....	17
3.3 Business Process Model and Notation .....	20
3.3.1 Alignment of BPMN to ISSRM Domain Model.....	20
3.4 Summary .....	23
CHAPTER 4. Security Risk Measurement .....	24
4.1 Security risk description with metrics .....	24
4.2 Measurement model within Misuse Cases .....	27
4.2.1 Metrics within Misuse Case Diagrams.....	27
4.2.2 SRMUC meta-model with metrics .....	29
4.3. Measurement model for BPMN .....	32
4.3.1 Metrics within BPMN diagrams .....	32
4.3.2 Metrics within BPMN meta-model .....	34
4.4 Summary .....	36
CHAPTER 5. Validation of Misuse Case and BPMN measurement models .....	38
5.1 Design.....	38
5.2 Participant selection .....	38
5.3 Visibility questionnaire .....	38
5.4 Results .....	39
5.3 Participants feedback.....	43
5.4 Threat to validity .....	44
5.5 Summary .....	44
CHAPTER 6. Conclusion and Future Work .....	45
6.1 Conclusion.....	45
6.2 Limitations .....	45
6.3 Future work .....	45
References .....	47
Appendix A. Survey .....	48
Appendix B. License .....	52

## List of Figures

Figure 1. ISSRM Domain Model, Mayer, 2009.....	13
Figure 2. Asset Modeling – MUC.....	18
Figure 3. Risk modeling – MUC.....	19
Figure 4. Risk Treatment Modeling – MUC.....	19
Figure 5. Asset modeling - sub-process Replace SEK to customer – BPMN.....	20
Figure 6. Asset modeling – sub-process Replace SEK to customer decomposed – BPMN...	21
Figure 7. Risk modeling – BPMN.....	22
Figure 8. Risk treatment modeling – BPMN.....	23
Figure 9. Introduction of metrics to misuse case diagram.....	27
Figure 10. Risk Reduction Level Calculation – MUC.....	28
Figure 11. Calculation of ROSI – MUC.....	29
Figure 12. MUC - business asset concept.....	30
Figure 13. MUC - vulnerability concept.....	30
Figure 14. MUC - security criterion concept.....	30
Figure 15. MC - threat and event concept.....	30
Figure 16. MUC - impact and risk concept.....	31
Figure 17. MUC - security requirement concept.....	31
Figure 18. Complete SROMUC meta-model.....	32
Figure 19. MUC – introduction of ROSI and RRL.....	32
Figure 20. Introduction of security need metric to BPMN diagram.....	32
Figure 21. Introduction of metrics to BPMN diagram.....	33
Figure 22. Risk Reduction Level calculation – BPMN.....	33
Figure 23. Calculation of ROSI – BPMN.....	34
Figure 24. BPMN – business asset and security requirement cost concepts.....	34
Figure 25. BPMN – vulnerability concept.....	35
Figure 26. BPMN – security need concept.....	35
Figure 27. BPMN – impact concept.....	35
Figure 28. BPMN – threat concept.....	35
Figure 29. Complete security risk-aware BPMN meta-model.....	36
Figure 30. BPMN - introduction of ROSI and RRL.....	36

**List of Tables**

Table 1. Quantitative evaluation scale.....14

Table 2. Qualitative evaluation scale.....14

Table 3. Misuse case diagram constructs aligned and extended to suit the ISSRM model....18

Table 4. BPMN graphical constructs aligned and extended to the ISSRM model.....21

Table 5. Examples of detected security risk cases.....24

Table 6. Threat likelihood scale.....26

Table 7. Total survey results.....39

Table 8. Cross-cut survey results.....40

Table 9. Evaluation of visibility of proposed metrics.....43

## ***Abbreviations***

IS	Information System
BPMN	Business Process Model and Notation
ISSRM	Information System Security Risk Management
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Edition
MUC	Misuse Cases
IT	Information Technology
ID	Identification
SEK	Sculpt Ergonomic Keyboard
SROMUC	Security Risk-Oriented Misuse Cases
RL	Risk Level
RRL	Risk Reduction Level
ROSI	Return on Security Investment
RM	Risk Mitigated
MAD	Mal-Activity Diagrams

## CHAPTER 1. Introduction

Rapid development of networks and computer-based information systems has given us great capabilities to process, store and transmit digital data in all business sectors. This development has raised a number of concerns about protection of organizational assets (Dhillon and Backhouse, 2000). Nowadays security concerns are mainly considered during the later phases of the development process and thus, lead to threat and vulnerability, which provide with a potential to exploitation of a risk (Soomro, 2012). Such approach also brings along higher spending on information systems security. The severity of security risks is not often visible in the early development stages. Introduction of metrics using modeling languages may bring this visibility of the severance of a risk.

Without knowing exactly how much damage an exploitation of a risk may bring it, is hard for management to make a decision about investments into security. The specialists of IS security must inspect possible threats and present the results together with cost and benefit of a particular security solution. This research deals with measurement of security risks using two modeling languages, aligned with security risk management – misuse cases (Soomro, 2012) and BPMN (Altuhhova, 2013). We will answer the following questions in the paper:

1. *How to introduce the security risk measurement into the Misuse Case and BPMN diagrams?*

To answer this question we first study metrics proposed by the author of ISSRM domain model (Mayer, 2009) for evaluation of business and IS assets, vulnerability, threat, impact, security criterion and security requirements. Mayer has followed the ISO/IES 27005 standard to adopt the metrics to his domain model. Secondly, we analyze misuse cases diagrams aligned to ISSRM proposed by Soomro (2012) and security-aware BPMN proposed by Altuhhova (2013). Both modeling languages provide a good visualization of a security risk itself, but do not give any measurement guidelines. In this research we apply a systematic approach to introduce measurement into two security-aware modeling languages in order to help evaluate the risk. To be exact, we divide the risk into sub-components and measure asset value, vulnerability level, threat likelihood, impact level, security need and security requirement cost. This will give us a possibility to calculate the risk reduction level and return on security investment, which is important for security specialists to understand whether investment into a particular security flaw is reasonable or not.

The second question that we will answer in the paper is:

2. *Which diagram extended with metrics (misuse cases or BPMN) is of higher visibility for its users?*

To answer this question we first develop a measurement model for security-aware misuse cases and for BPMN. Then a questionnaire is composed to validate the visibility of two models. Based on the survey, conducted among to groups of people, first who are aware of a security risk described and second, who are familiar with modeling languages, we plan to get the answer to the stated question. Results of the survey will be evaluated in two ways. First of all we will analyze answers from all participants in total. Then the results will be cross-cut and each question will be weighted. This will give us deeper understanding about the visibility of a particular metric.

The thesis is divided into six chapters. *Chapter 1* gives an introduction to the research questions and the motivation for the work. Main background knowledge is presented in *Chapter 2*. We give an overview of existing security risk management standards and methods. Moreover, ISSRM domain model is studied in greater details as it provides metrics which are

later reused in the paper. *Chapter 3* describes two security risk-aware modeling languages: misuse cases and BPMN. We illustrate the languages through an IS replacement by drawing diagrams. The security risk is taken from a functional organization. In *Chapter 4* we develop two measurement models. First, we divide the risk into sub-components and measure them. Next, we introduce these measurements into misuse cases and BPMN diagrams. Two derived metrics such as risk reduction level and return on security investments are calculated in this chapter. *Chapter 5* validates two measurement models. The chapter discusses in which model it is easier to identify expressions of metrics. We also investigate threat to validity of the results. The last *Chapter 6* summarizes the research results and discusses possible future work.

## **CHAPTER 2. Approaches for Security Risk Management**

The literature study of the second chapter of this paper consists of an overview of security risk management in general. Then it is followed by the presentation of existing risk management standards and methods in order to gain basic guidelines about risk assessment process. Finally, one security risk management approach will be chosen for further use.

### ***2.1 Introduction to security risk management***

Security risk management is the process that provides guidance on how to minimize the risk level of intentional and undesirable events that may affect business assets (Talbot and Jakeman, 2009). It is a first priority for a management team to secure any business from operational risks. The impact from losses of life, intellectual property, physical assets and reputation can be dramatic for business. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty.

The core components of any security risk management process (Jenkins, 1998) are the following:

- Company assets identification;
- Value assignment to each asset;
- Vulnerability identification for each asset;
- Risk calculation for identified assets;
- Selection of countermeasures to mitigate the calculated risks.

There are various approaches, techniques, methods and standards available for managing organizational risks. As an example following methods can be mentioned: CORAS (Soldal et al, 2011), OCTAVE (Alberts and Dorofee, 2003), CRAMM (Neubauer, 2009), ISSRM (Mayer, 2009), etc. Besides multiple methods and approaches, there are also standards that describe risk management process and serve as a guide for them. Major standards will be reviewed and compared to the core components of a security risk management.

### ***2.2 Standards***

Different standards give guidelines how security risk management should be conducted, but they do not state which a security management approach should be used. Two standards, recognized and used worldwide are reviewed – ISO (ISO, 2005 and 2008) and NIST (NIST, 2012).

ISO is the International Organization for Standardization that develops and publishes international standards. The paper focuses mainly on the ISO 27000 which is a family of standards that helps organizations to keep information assets secure.

NIST (National Institute of Standards and Technology) is a federal technology agency founded by the U.S. Department of Commerce that has a mission to develop and promote measurement, standards and technology. The series of NIST SP 800 present the most interest in this paper which deal with computer security and particularly describe the risk assessment approach.

### ISO Standards

The objective of ISO/IEC 27001 (ISO, 2005) is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving ISMS. The standard adopts the Plan-Do-Check-Act model, applied to all security risk management processes which requires management in an organization in order to examine security risks systematically, address them and ensure security controls, continue to meet the security needs. ISO/IEC 27001 describes the process of risk management as follows: asset identification, threat identification, vulnerability identification that might be exploited by the threat, impact identification, risk analysis and evaluation, risk treatment, selection of controls. According to the standard, each organization should define the risk management approach that will best suite the requirements of the business.

The information security risk management process and its activities are outlined in the ISO/IEC 27005 (ISO, 2008). This standard supports the general concepts, specified in ISO/IEC 27001, and illustrates the information security risk management process: context establishment; risk assessment; risk treatment; risk acceptance; risk communication; risk monitoring and review.

### NIST 800-30rev1

NIST 800-30rev1 (NIST, 2012) is entitled „Guide for Conducting Risk Assessments”. Its main objective is to provide guidance for conducting risk assessments of information systems. The main targets of series NIST 800 are federal organizations that process sensitive information. However, the proposed guidelines may be applied by non-governmental organizations as well.

According to the special publication, risk assessment is one of the fundamental components of an organizational risk management process as described in NIST Special Publication 800-39 and can be conducted at all risk management levels(organizational, mission/business process and information system level). The process of conducting the risk assessment in an organization, depicted in the standard, includes 4 steps:

- Prepare for assessment – identify purpose, scope, assumptions and constraints, information sources, risk model and analytic approach;
- Conduct assessment – identify threat sources, threat events, and vulnerabilities and predisposing conditions; determine likelihood, impact, risk;
- Communicate results – communicate risk assessment results, share risk-related information;
- Maintain assessment – monitor risk factors, update risk assessment.

## **2.3 Security risk management methodologies**

While standards give general guidelines of how security risk management should be implemented, various approaches may give practical techniques of implementation.

Frameworks of CORAS (Soldal et al, 2011) and CRAMM (Neubauer, 2009) are centered on traditional risk assessment process, providing step by step procedure, described above. CORAS consists of a language, a tool and a method. The method stresses the importance of a risk modeling and the need to analyze what can go wrong. Its risk management process consists of the following steps:

- Establish Context;
- Identify Risks;
- Analyze Risks;
- Risk Evaluation;
- Risk Treatment.

The security risk management presented in CRAMM (Pantaziz, 2011) consists of the following steps:

- Evaluation of the scope of security;
- Evaluation of the risk;
- Selection of countermeasures.

OCTAVE (Alberts and Dorofee, 2003) is quite different – it provides a set of criteria containing guidelines and requirements for implementing process steps, instead of pre-specified techniques, thus can be adapted to any organization. It is based on the self-direction approach, which means that the process should be conducted by internal employees.

The ISSRM (Mayer, 2009) method, as well as all above mentioned approaches, covers the general risk assessment process. The major differences in various methods can be found in the manner of approach to its components.

For the further research we will concentrate on ISSRM concept. It suggests the process guidelines to help identify the vulnerable assets, determine their security objectives, assess the risks, and elicit security requirements to mitigate these risks (Altuhhova et al., 2012). But the major benefit is that the domain model covers metrics for security risk assessment. These metrics can later be used in the paper. Besides that, an extensive analysis of alignment of ISSRM domain model and misuse cases so as BPMN, on which the paper is based on, was conducted. It may aid in the development of security risk measurement models.

## **2.4 ISSRM domain model**

Information system security risk management (ISSRM) domain model is a framework which addresses security related issues in an information system domain (Mayer, 2009). The domain model was defined after a careful survey of the risk management standards, security related standards, security risk management methods and software engineering frameworks. ISSRM activities follow an overall process of security risk management and consist of the following steps (Mayer, 2009): Context and asset identification, determination of security objectives, risk analysis and assessment, risk treatment, security requirements definition, control selection and implementation.

The focus of ISSRM domain model is to secure the information system. The model is composed of three conceptual categories (Mayer, 2009): asset-related concepts, risk-related concepts and risk-treatment related concepts, shown in Figure 1.

### **2.4.1 Asset-related concepts**

The goal of the concepts is to define and secure the assets that have some value for the organization and detect the security criteria of those assets. *Asset* is something that has value to the organization and supports the achievement of organizations' objectives. *Business asset* is an information or process that has some value and aid to achieve objectives of an organization. *IS asset* is a part of an IS that has some value and supports the business asset.

*Security criterion* is property on business assets that characterizes their security needs. It usually consists of confidentiality, integrity and availability, but can be extended to non-repudiation and authenticity (Matulevičius et al, 2008).

## 2.4.2 Risk-related concepts

Concepts describe which components should be taken into account while defining the risk. *Risk* is a combination of event and the consequences of an impact, caused by exploiting some vulnerability. *Impact* is negative results, caused by the event. *Event* is a result of a combination of a threat and one or more vulnerabilities. *Vulnerability* is some weak link in an information system that can be targeted either intentionally or accidentally. *Threat* is an incident, performed by a threat agent who attacks multiple IS assets, using some attack method and targeting to harm the business asset. *Threat agent* –is someone who can cause a threat into a business asset. *Attack method* is a method used by a thread agent in order to perform a threat (Matulevičius et al, 2008).

## 2.4.3 Risk-treatment related concepts

Concepts state which security requirements or controls need to be implemented in order to better mitigate or avoid the potential risk.

*Risk treatment* is a decision on dealing with the potential risk, reducing it, transferring, avoiding or accepting. *Security requirement* is a detailed countermeasure to mitigate the potential risk. *Control* gives guidelines on how to mitigate the potential risk (Matulevičius et al, 2008).

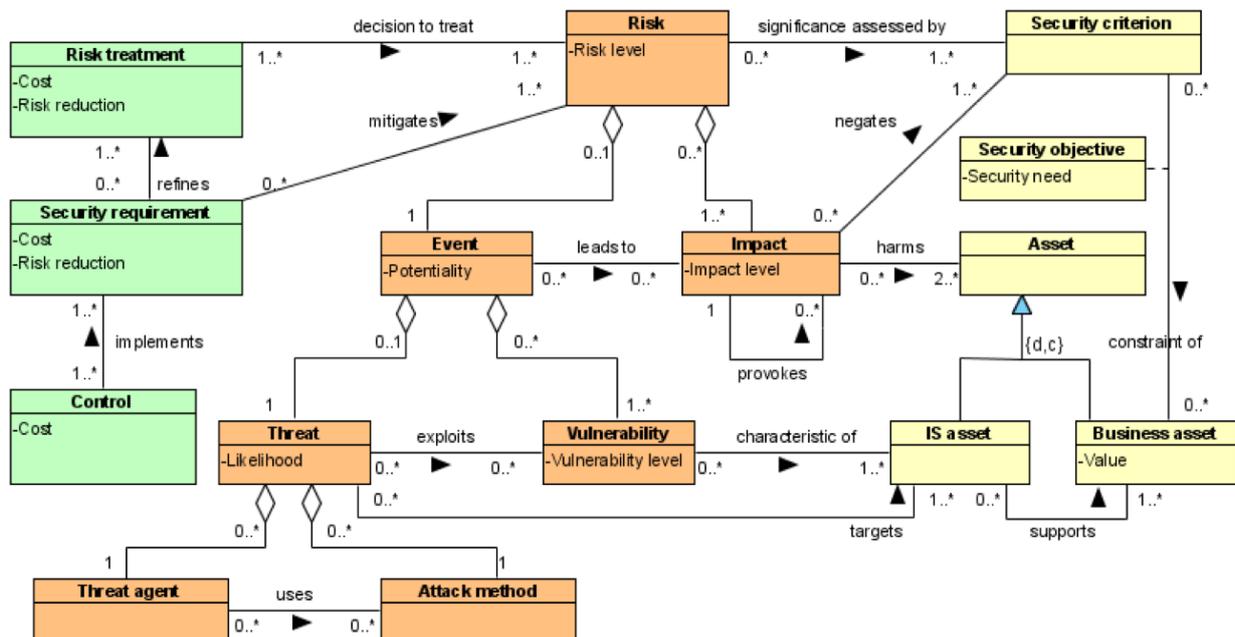


Figure 1. ISSRM Domain Model (Mayer, 2009)

## 2.4.4 ISSRM metrics

There are two basic methods to evaluate the risks; the subjective method (qualitative, quantitative, semi-quantitative risk estimation) and the objective method. Both of them are valid.

*Quantitative risk analysis* typically employs a set of methods or principles for assessing risks, based on the use of numbers. It tries to assign hard financial values to assets, expected losses,

and cost of controls. This method gives the most accurate data, but quantitative risk analysis requires significant amount of information and time and can be applied only in specific situations (Shimonski, 2002). The example of quantitative scale is shown in Table 1.

Table 1. Quantitative evaluation scale

Consequence in €	Likelihood	Level
50 000	1	1
5 000	0.1	2
500	0.01	3
50	0.001	4
< 5	0.0001	5

*Qualitative risk analysis* typically employs a set of methods or principles based on non-numerical categories or levels (e.g., very low, low, moderate, high, very high). The basic process for risk assessment of qualitative approach is similar to what happens in the quantitative approach. The main difference between quantitative and qualitative approaches is that the latter one calculates relative values and do not invest a lot of time, trying to calculate precise financial numbers for asset valuation, possible impact from a risk being realized and the cost of implementing controls (Mayer, 2009). Examples of qualitative scales are shown in Table 2.

Table 2. Qualitative evaluation scale

Consequence	Likelihood	Level
Very high	Certain	1
High	Likely	2
Medium	Possible	3
Low	Unlikely	4
Very low	Rare	5

The benefits of the qualitative approach are that it is much less demanding on staff, requires less time and information. Results can already be seen in couple of weeks. The drawback of a qualitative approach is that the results are vague and imprecise because of the relative values determined during a qualitative risk assessment project.

*Semi-qualitative risk analysis* gives more precise results than from qualitative approach; however, the estimation remains less accurate than with quantitative (Mayer, 2009).

One of the most notable things about ISSRM model is that it provides metrics for risk, business asset, security objective, impact level, event potentiality, threat likelihood and vulnerability level evaluation. In case a risk level is considered to be unacceptable, metrics for risk treatment, security requirements as well as controls are suggested.

Authors of the ISSRM domain model (Mayer, 2009) offer a concrete implementation of each metric proposed: *Business asset value* is qualitative estimation, offering three levels: normal, high and very high. A very high value of a business asset directly concerns the authenticity process or has a great importance for the client has. A high value has an asset concerning the clients of an organization. An asset with normal value concerns only the internal functioning of an organization, having no direct relation with the customers. *Security objective* is a qualitative scale of four, defined for confidentiality, integrity and availability and representing the level of security need. Levels 1 to 3 are defined in accordance with the business asset

value scale; whereas level 0 states that there is no need in security at all. *Threat likelihood* is a qualitative scale going from 1 to 3 as estimated. The first level depicts threats that are unlikely to happen, which means they can happen rarely. The second level includes threats that can happen sometimes, but not very often. The last third level is about threats that are very likely to happen since no particular investments or competencies are needed to perform this threat. *Vulnerability level* has a qualitative scale of four from levels 0 to 3. Level 0 means that the vulnerability level is very low and security measures are in place; level 1 means that security measures are insufficient or not adapted to the situation; level 2 represents that no sufficient security measures are in place and level 3 means that no security measures are implemented or they are out of date. *Event potentiality* is calculated as a summary of a threat likelihood and vulnerability level minus 1. Since not each threat will lead to the impact and harm business asset, a scale of three is determined to represent the *Impact level*. It shows how many security criteria are negated. Risk level is a matrix of event of potentiality and impact level. Author of an ISSRM domain model suggests that each organization should determine which levels of risk should be defined as acceptable and intolerable. *Risk treatment* is a choice between risk reduction, transfer or avoidance. *Security requirements* are defined according to the situation with the respect to mitigate discovered vulnerabilities. *Control costs* are defined in terms of financial data.

Metrics introduced in this section will be later applied to extend misuse case and BPMN diagrams.

## **2.6 Summary**

Today IT risk and information security are regarded as business issues but not only technical ones. The whole organization requires being aware of possible risks and following the risk management procedures in order to keep business assets secured.

Security risk management has developed a lot of different approaches, methods and standards in order to manage the risk at the requirement elicitation phase. ISSRM domain model was developed from the existing models and standards. In our work we have selected ISSRM domain model, suggesting help to identify assets and risks, select security requirements and mitigate risks. We have decided to carry on with using this model because, first of all, ISSRM covers the security risk management concepts at three conceptual levels. Secondly, different modeling languages have been aligned to them. Finally, ISSRM model has introduced metrics which later may be introduced to misuse case and BPMN diagrams.

## CHAPTER 3. Security Risk-Oriented Modeling

Chapter three will first introduce the description of a security risk. Then such modeling languages as misuse cases and BPMN will be described using the given security risk example. Finally, we will illustrate how two modeling languages are interpreted with respect to the previously chosen ISSRM concepts.

Security engineering concentrates on tools, processes and methodologies that support analysis, design and implementation of new systems or adjusting existing system according to the needs of its environment (Altuhhova, 2013). Security engineering is concerned about lowering the risk of intentional harm to valuable assets to the level that is acceptable to the system's stakeholders (Matulevicius, 2014). However, the literature reports that security concerns often arise only during the implementation or maintenance of the actual system. Early security consideration could help developers to elicit security threats, their consequences and design countermeasures without suffering from high costs.

Modeling languages provide powerful means to understand the security concerns during the early system development stages. There are different studies that focus on security risk management for IS requirements engineering. For example, Mal-activity Diagrams (Chowdhury, 2012), Misuse Cases (Sindre and Opdahl, 2002) and BPMN (Altuhhova, 2013). These modeling languages were aligned to ISSRM domain in purpose to understand how they deal with security. In this chapter we will introduce two modeling languages such as misuse cases and BPMN with the help of the risk described below. This will bring us to the next chapter, where the metrics will be aligned to those modeling languages, using the data from our security risk example.

### **3.1 Security risk description**

The organization provides services for replacement of broken or damaged hardware parts within a warranty period (e.g. mouse, keyboard, web-cam). If a customer purchases a hardware part and discovers that it is not working, he may apply for free of charge replacement online. To do that a customer needs to fill in an online form with his personal data and provide a product ID of a broken hardware part. First, an employee of a technical department receives the replacement request and registers it into the system. The product ID is used by the employee to determine which part of hardware a customer wishes to replace. Then an employee of a fulfillment department views the registered request (customer shipping information and the name of a product are visible) and places the order to replace that product. Finally, the hardware part is shipped out to the customer from a warehouse free of charge.

The risk imposed to that process is that a person may apply online request for hardware replacement without previously buying the product. For this it is only needed to find a product ID on the Internet, fill out the online form and receive the hardware free of charge. The organization has been suffering from that risk for several years now. Some countermeasures were implemented, but they prove to be not very efficient. It is still a big concern for the company since a lot of information can be found in forums about ways of cheating the system. Our goal is to illustrate the security risk using two modeling languages such as misuse case diagrams and BPMN. Later in the paper metrics into them will be introduced in order to better understand the severity of a security risk. The language

introduction will be based on the replacement of Sculpt Ergonomic Keyboard – one of the items that can be replaced by the organization.

### **3.2 Misuse cases**

Misuse cases is a modeling tool in requirements engineering field that helps to determine security requirements, since use cases have limited support for eliciting them. Positive use case diagrams were extended with negative use cases or misuse cases that specify behavior not wanted in the proposed system (Sindre et al., 2004). Misuse case describes the process of executing a malicious act against a system, while use case describes any action taken by the system.

Misuse cases include both the graphical and textual notations. A misuse case diagram is presented together with the use case diagram. In addition to the definitions of use case and actor, two new entities are introduced (Sindre et al., 2004) such as *misuse case* which is a sequence of actions performed in order to harm the system and a *misuser* which is the actor that initiates the misuse case either intentionally or inadvertently. In addition, new relationships are introduced by misuse cases such as *mitigate* when the use case reduces the chance of a misuse case to succeed and *threaten* when a misuse case can hinder a use case to achieve its goals. Such relationships as *include*, *extend* and *generalize*, found in use case models and are used between misuse cases too. Misuse cases also include a concept of *vulnerability* as a weakness of a system (Soomro et al., 2013). Besides the diagram, the essence of a misuse case is captured in the associated textual description. These templates encourage developers to write clear action steps. There are two ways to express misuse case textually: lightweight description, which is better for early development stages and an extensive description, which is better for later development stages. These textual descriptions will not be analyzed in our further work; we will focus only on the MUC diagrams.

The process for eliciting security requirements with misuse cases proposed by Sindre et al.(2013) follows five steps:

Step 1: Identification of critical assets.

Step 2: Definition of security goals.

Step 3: Identification of threats – threats can be described both as misuse cases and misusers.

Step 4: Identification and analysis of risks – the identification of extend/include or generalization relationships between misuse cases can aid risk analysis.

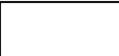
Step 5: Definition of security requirements - can be specified either as an independent security use cases or in the mitigation fields of extensively described misuse cases.

First, the analysis of misuse cases showed that they do not comply with security risk management strategies since misuse cases lack several constructs to address secure assets, security risks and their countermeasures (Soomro et al. 2013). Later on, Soomro and Ahmed proposed few improvements to the misuse case diagrams by aligning their constructs with the concepts of ISSRM domain model. The missing semantics were introduced into the language. Graphical constructs of misuse cases are presented in Table 3.

#### **3.2.1 Alignment of misuse cases to ISSRM Domain Model**

We will illustrate the application of security risk-oriented Misuse Case (SROMUC), using the security risk introduced above. The result of alignment of misuse cases with ISSRM domain model (Soomro et al. 2013) is illustrated in Figures 2, 3 and 4, using a security scenario on asset integrity.

Table 3. Misuse case diagram constructs aligned and extended to suit the ISSRM model

ISSRM domain model	Misuse case diagrams
Assets/ Business assets	 Actor  Use case
IS assets	 System  Use case
Security criterion	
Impact	
Vulnerability	
Attack method	 Misuse case
Threat agent	 Misuser
Security requirement	 Security use case

**Asset model** in Figure 2 illustrates the context of a Sculpt Ergonomic Keyboard (SEK) replacement IS in a use case diagram. This case is focused on SEK replacement IS integrity. A security criterion is a security constraint imposed on business asset – *SEK replacement to customer*, which extends to IS assets – *register request to replace SEK and ship out the product*. The example focuses on the employee and a customer who communicates with SEK replacement IS. The employee and the customer are assets characterizing the users of the system in reference to ISSRM domain model. A customer seeks to *submit the online request to replace SEK with valid ID* and receive the SEK free of charge. The employee seeks to *replace SEK to the customer*.

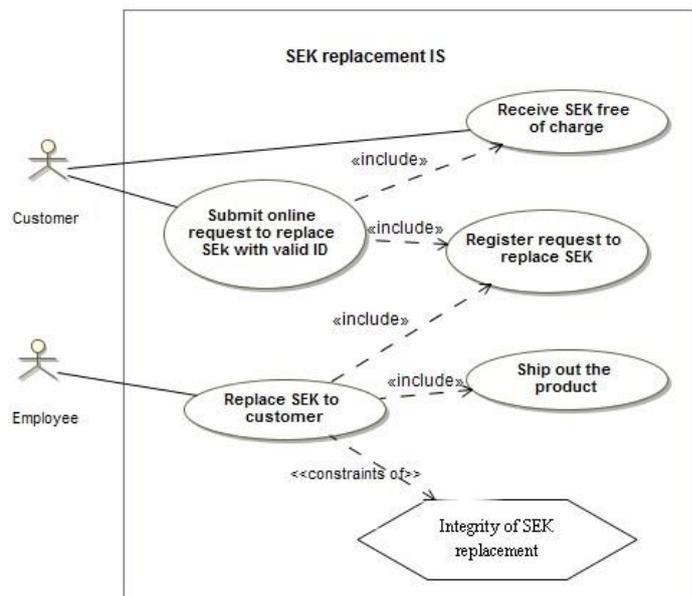


Figure 2. Asset Modeling - MUC

**Risk model** in Figure 3 illustrates the potential security threat scenario. A misuser or in our case a non-legitimate customer initiates a misuse case - *submit the online request to replace SEK using the product ID found on the Internet* by exploiting the vulnerability - *poor check of product IDs* in a use case which leads to the use case - *receive SEK free of charge* in the end. This vulnerability is represented by a use case painted in gray. The threat *online request to replace SEK with product ID found on the Internet* leads to an impact - *loss of reliability of replacement process* which harms the business use case - *replace SEK to customer* and dis-affirms the security criterion *Integrity of SEK replacement*.

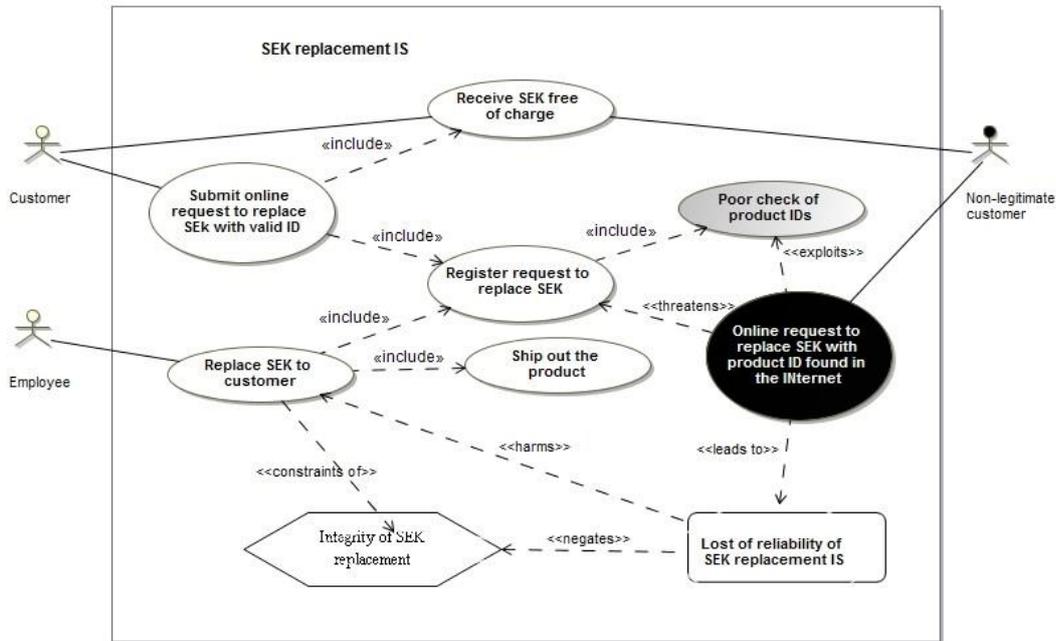


Figure 3. Risk modeling - MUC

**Risk treatment model** shown in Figure 4 does not support the modeling of risk treatment, control and its implementation as the ISSRM domain model defines them. Instead of this the security requirement is illustrated as a security use case. The security use case is represented as a use case with a lock inside. The IS asset – *register the request to replace SEK* includes one security use cases - *request for different proof of purchase-invoice*. The security use case mitigates the misuse case - *online request to replace SEK with product ID found in the Internet*. It ensures security criterion *Integrity of SEK replacement* imposed by a business use case - *replace SEK to customer*.

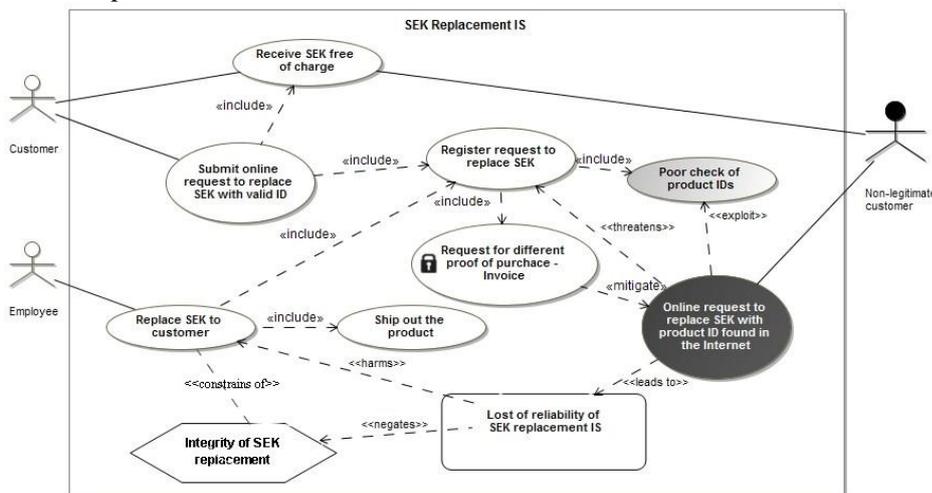


Figure 4. Risk Treatment Modeling - MUC

### 3.3 Business Process Model and Notation

The Business Process Modeling Notation is a standard to model business process flows and web services with a goal to provide a notation that can be understood by all business users (Owen and Raj, 2003). BPMN is a language for constructing business process models based on notions familiar to traditional flowcharts. The key element of BPMN application is the Business Process Diagram. It consists of a set of various graphical elements that are familiar to most modelers (Altuhhova et al, 2012). It describes a typical order of activities and what role an organizational unit performs in the process. Initially BPMN was not designed to cover security risk management, but it was later extended (Altuhhova, 2013) to follow the risk management guidelines, which will be illustrated later in the paper.

BPMN modeling is divided into three levels: analytical, executable and descriptive modeling. We are only looking into descriptive modeling, which concentrates on major business flows. Graphical constructs of a descriptive modeling are introduced in Table 4.

#### 3.3.1 Alignment of BPMN to ISSRM Domain Model

To illustrate how the security risk management is addressed using BPMN language, we will present an example related to integrity of the replacement process for Sculpt Ergonomic Keyboard. This is the same security risk which was analyzed, using misuse case diagrams given above.

For **asset-related concept** Altuhhova (2013) observes that in the concept of ISSRM the *pool*, *lane* and *data store* in BPMN describe the information system asset. The BPMN constructs like *task*, *gateway*, *event* and their connecting links help describe business asset in terms of ISSRM concept. The BPMN *data object* is aligned to the ISSRM business asset as well. Such visual element as *lock* is used to express ISSRM security objective.

Altuhhova et al. (2012) proposes to use visual variables for the modeling language. Black color is used for asset modeling that is presented in Figure 5. The case is focused on SEK replacement IS integrity. A security constraint - *integrity of SEK replacement* is imposed on business asset - *replace SEK to customer*. A customer, user of a system, seeks to place an *online request to replace SEK with valid ID* in order to receive SEK free of charge. Figure 5 illustrates the sub-process of SEK replacement IS, whereas Figure 6 illustrates a decomposed process for SEK replacement IS.

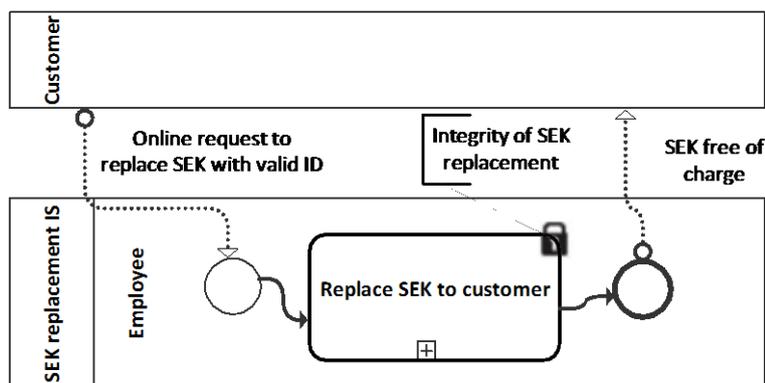


Figure 5. Asset modeling - sub-process Replace SEK to customer – BPMN

On Figure 6 we can see that the business asset - *replace SEK to customer* is extended to IS assets – *register request to replace SEK and ship out the product*.

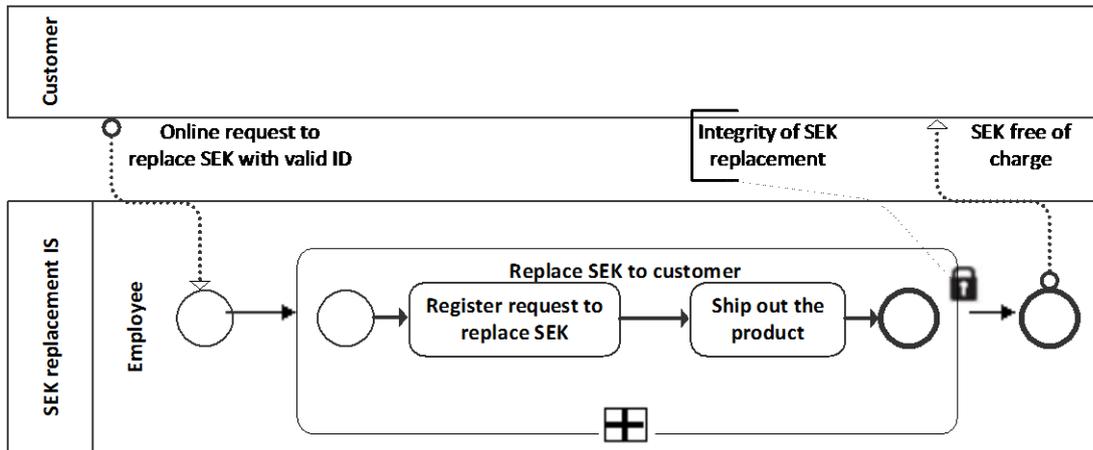


Figure 6. Asset modeling – sub-process Replace SEK to customer decomposed - BPMN

Table 4. BPMN graphical constructs aligned and extended to the ISSRM model

ISSRM domain	BPMN constructs
Assets	   Task                      Event                      Gateway
Business assets	 Data object
IS assets	  Pool                      Data store
Security criterion	
Impact	
Vulnerability	
Attack method	   Task                      Event                      Gateway
Threat agent	
Security requirement	   Task                      Event                      Gateway

For **risk-related concept** the risk related constructs are presented in red, as proposed by Altuhhova et al. (2012). BPMN *pools* and *lanes* represent the ISSRM threat agent; and the ISSRM attack method is expressed in a combination of *event*, *gateway* and *task*. Vulnerability in BPMN is a characteristic of IS asset and it is represented using *annotations*. Threat is introduced as a combination of BPMN constructs used to model the threat agent and attack method. Event in turn is expressed as a combination of threat and vulnerability. Altuhhova et al. (2012) suggests to express impact through the *unlock* symbol.

A threat - *online request to replace SEK with product ID found in the Internet* is initiated by an attack agent - *non-legitimate customer*. The vulnerability - *poor check of product IDs* of an IS asset - *register request to replace SEK* is exploited and which leads to an impact. As a result a non-legitimate customer receives SEK free of charge along with the valid customer. See Figure 7.

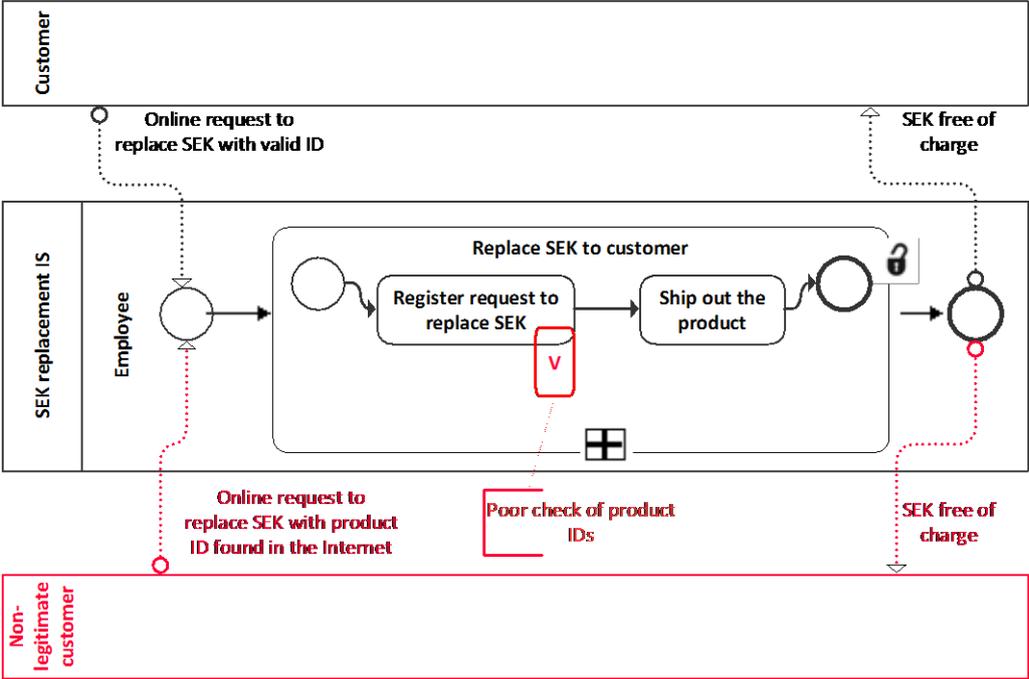


Figure 7. Risk modeling - BPMN

For **risk treatment-related concept** risk treatment constructs are presented in blue (Altuhhova et al., 2012). The ISSRM security requirements and mitigation relationship are introduced by the combination of *flow objects*. Such ISSRM constructs as risk treatment and security control are not expressed in BPMN.

Security requirement - *request for different proof of purchase – invoice* on Figure 8 mitigates the imposed threat *online request to replace SEK with product ID found on the Internet* by not allowing a non-legitimate customer to receive SEK free of charge.

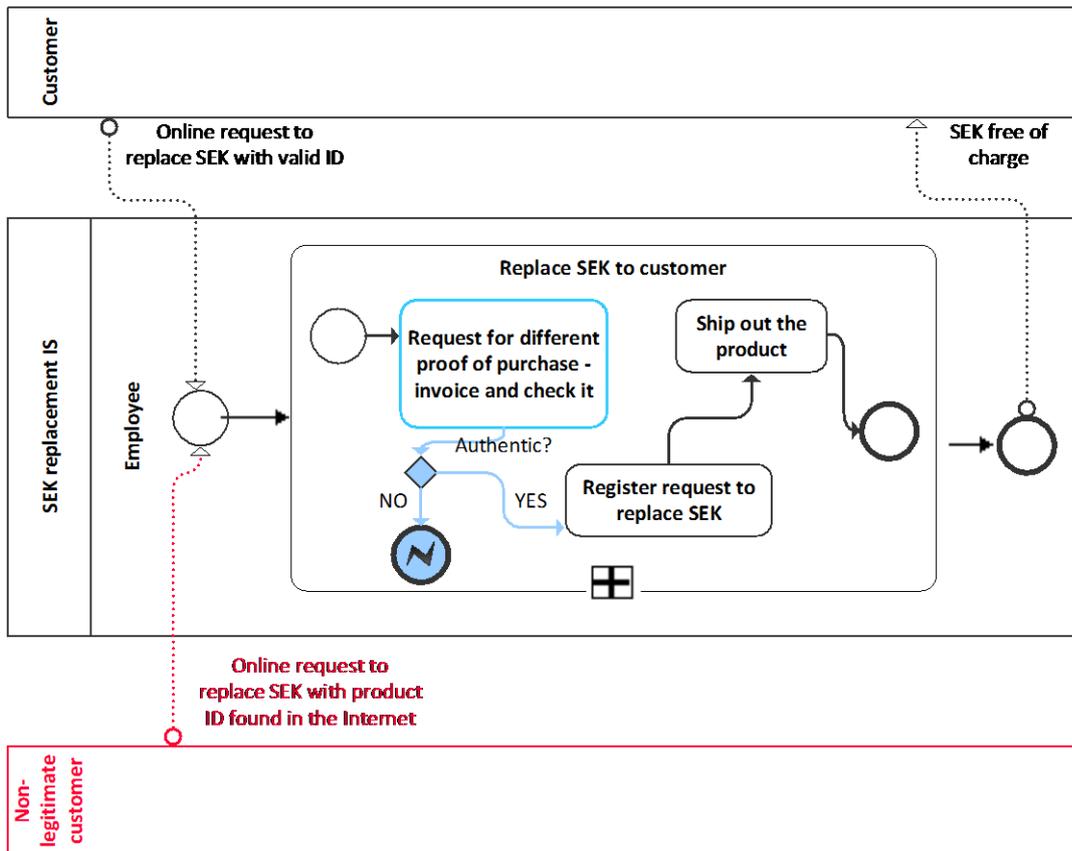


Figure 8. Risk treatment modeling - BPMN

### 3.4 Summary

In this chapter we have covered two modeling languages – misuse case diagrams and BPMN and introduced their alignment to ISSRM domain model, using the security risk example taken from a real world environment. When illustrating the security risk, using two modeling languages, we were able to introduce such ISSRM constructs as business asset, IS asset, security criterion, vulnerability, threat, impact and security requirement. Such ISSRM constructs as risk treatment and control appeared not to be expressed by both misuse cases and BPMN. The diagrams used to model the security risk example with the help of misuse cases and BPMN modeling languages will be extended with metrics in the next chapter.

## CHAPTER 4. Security Risk Measurement

In this chapter we first present the security risk example from a real world environment together with quantitative data. Then based on the metrics suggested by the ISSRM model and using our collected data we measure asset value, vulnerability level, threat likelihood, impact level, security need and security requirement cost. Those values will be introduced in the misuse case and BPMN diagrams. This will help us to calculate the risk level, risk reduction level and return on security investment, which in turn will facilitate to evaluate the severances of a present risk. It will give management a clear picture whether the risk should be fixed.

### 4.1 Security risk description with metrics

In order to see how much damage the risk is generating to the company we will take some quantitative data that shows how many security risk cases were detected for the last year and how much each item costs. See Table 5. There were in total 150 replacement requests last year, 20 out of them were detected as fraud cases. The last column indicates percentage of security risk cases out of total order replacement requests. This data will be used in order to introduce metrics into two modeling languages.

Table 5. Examples of detected security risk cases

Item Name	Price in EUR	Total replacement orders	Amount of detected fraud replacement orders	% of fraud replacement orders
SideWinder Keyboard X4	70	4	1	25%
SideWinder Keyboard X6	80	23	7	30%
Presenter Mouse	80	3	1	33%
Wireless Comfort Desktop	80	10	1	10%
Wired Intellimouse	80	5	1	20%
Mobile Memory Mouse	80	9	1	11%
Comfort Desktop 5000	80	13	1	8%
Ergo Desktop 7000	90	13	1	8%
LifeCam Studio	100	3	1	33%
SideWinder Mouse X8	100	8	1	12%
Wireless Laser Desktop	120	11	1	9%
<b>Sculpt Ergonomic Desktop</b>	<b>140</b>	<b>14</b>	<b>1</b>	<b>7%</b>
Enterprise Desktop 7000	300	5	1	20%
Enterprise Desktop 8000	400	4	1	25%
Other items	70-400	24	0	0%
Total orders:		150	20	

We will take one example of the security risk from Table 5, marked in red, and look at it in greater details – replacement order for Sculpt Ergonomic Keyboard (SEK). Below we will

identify business and IS assets of the organization; define the security criterion and risk, which is composed of a threat, vulnerability, impact and event. Threat agent and threat method will be also identified. Finally, we will define security requirements and controls. For all those constructs values will be assigned based on the ISSRM model. The data for assignment of values will be partly taken from Table 5.

**Business asset** – replacement order for Sculpt Ergonomic Keyboard.

*Importance* – since the business asset is supported by various information system (IS) assets, we may calculate the total asset value under this construct. The cost for replacement of Sculpt Ergonomic Keyboard consists of the item price and its shipping and handling costs which makes it 140 euro for the product and approximately 30 euro for shipment. This gives us the total asset value of 170 euro.

**IS asset** – order replacement tools.

*Importance* – following the concept of ISSRM domain model the value of IS assets are not taken into consideration, when calculating the total asset value. One of the main reasons is that IS asset may support different business assets, thus, have different values and security needs. Moreover, we have observed that prices for maintenance and usage of the tools during replacement process are fixed and do not change from case to case.

**Security objective** -metrics proposed by the authors of an ISSRM domain model may be applied. It means that a scale of four is defined for confidentiality, integrity and availability for representing the level of security need. Levels 1 to 3 are defined in accordance with the intangible business asset value, whereas level 0 states that there is no need in security at all.

C – Confidentiality of the replacement process of SEK should be at level 2. The general replacement process should be known to end customers, keeping its details confidential.

I – Integrity of the replacement of SEK is ranked at level 3. The replacement process should stay non-altered.

A – Availability of replacement option should be at level 3. Customer satisfaction is of high priority for the company, therefore, replacement should always be available to customers and the process itself should be easy and quick.

**Threat agent** – non-legitimate customer – a customer who has not initially purchased the hardware and wants to “replace” it.

*Importance* – the value of a threat agent in general depends on its loss and gain. The more competencies the attack is required, the more dangerous and expensive it is to the attacker, the less the likelihood of the threat is. It is not calculated independently but as a part of the total threat value.

**Attack method** - product ID is found on the Internet (e.g. forum) and submitted together with the replacement request.

*Importance* – the value of the attack method depends on its complexity. It is taken into consideration while determining the total threat value, which does not have its own metrics.

**Vulnerability** - easy to find the product ID on the internet and poor, almost non-existing check of product IDs.

*Importance* - A scale of three may be used in order to measure how vulnerable is the system to a threat. In our example the vulnerability level has the level of 2, since there is a very poor process for product ID check is implemented. The product ID is used to determine which product to replace for the customer instead of checking whether the product was previously purchased or not.

**Threat** – a non-legitimate customer submits the order replacement request online for SEK using a product ID found on the Internet and receives the free of charge hardware.

*Importance* – threat likelihood may be calculated based on the data we have in Table 5. During the last year there were about 14 cases of replacement of SEK, one of them was detected as a fraud case. So the threat likelihood is calculated to be 7%. In order to calculate further the risk level we need to standardize the value of threat and vulnerability. We have chosen to measure those two constructs in terms of level, as suggested by the ISSRM model. We can see from Table 5 that the highest percentage rate of security risk cases is 33% and the lowest is 0%. Based on that we came up with the following scale:

Table 6. Threat likelihood scale

Threat likelihood in %	Level of threat likelihood
0% - 10%	1
Above 10% - 21%	2
Above 21%	3

Thanks to Table 6 threat likelihood is now has the same relative metrics as vulnerability level, and has the value of 1. Moreover, our value for threat likelihood is less subjective now.

**Impact:**

- harms the product replacement process by slowing down the work of employees and bringing the financial loss;
- the online SEK replacement tool is not reliable anymore as it cannot tell whether a customer is eligible or not;
- negates the integrity of a product replacement, meaning the business asset is not reliable and correct;
- leads to substantial loss to a company by providing too much orders to non-legitimate customers.

*Importance* - the impact level in our case is determined to be 3 on the scale of 3. The reason for this is that the threat negates the security criterion which is integrity of the replacement process for SEK, and has the highest value of 3 as well.

**Event** – a person without initially purchasing the hardware places the replacement request by finding a product ID on the Internet.

*Importance* – following the ISSRM domain model guidelines the event represents the combination of threat and vulnerability. We calculate the event potentiality by summarizing a threat likelihood and vulnerability level and minus 1 (1+2-1=2). So we get an event potentiality of 2.

**Risk** – a person who did not previously purchase the hardware places a replacement request online with a product ID that was found on the Internet due to the availability of such information and poor check of Ids, so receives the free of charge hardware from a company. It leads to the loss of integrity and, thus, reliability of the SEK replacement process.

*Importance* – the risk level is represented by the combination of event and impact and will be discussed in greater details below.

**Risk treatment decision** – risk avoidance.

*Importance* – the value is determined in final control cost calculation; no measurements are presented at this point.

**Security requirement** - stop accepting product ID as a reliable proof of purchase, request invoice from the store instead.

**Importance** – cost of security requirement is presented in EUR. The total cost of the solution will be approximately 200 euro for the change of the IS replacement system to start accepting invoice as a proof of purchase. This change includes the work time of employees who will be involved in the change of system configurations. Implementation of this security requirement will avoid all security risks. In total we have detected 20 risks, but since we are looking only at one risk, solution costs need to be adjusted as well. If we divide total cost by all security risk cases, we get the cost for our one risk scenario (200EUR / 20 = 10EUR).

**Control** - request customers to provide more reliable proof of purchase, for example, a copy of receipt from the store by reconfiguring the system parameters.

**Importance** – control costs are defined in terms of financial value, but they are not covered by misuse cases, therefore, we are not defining them for our further work.

## 4.2 Measurement model within Misuse Cases

In this chapter we will introduce metrics within misuse case diagrams and meta-model. Two different viewpoints on metrics will be presented such as risk reduction level and return on security investment. This will give us better understanding whether it is reasonable to mitigate the risk or not.

### 4.2.1 Metrics within Misuse Case Diagrams

Now when all values for constructs are identified above, we need to align them with a misuse case diagram. See Figure 9.

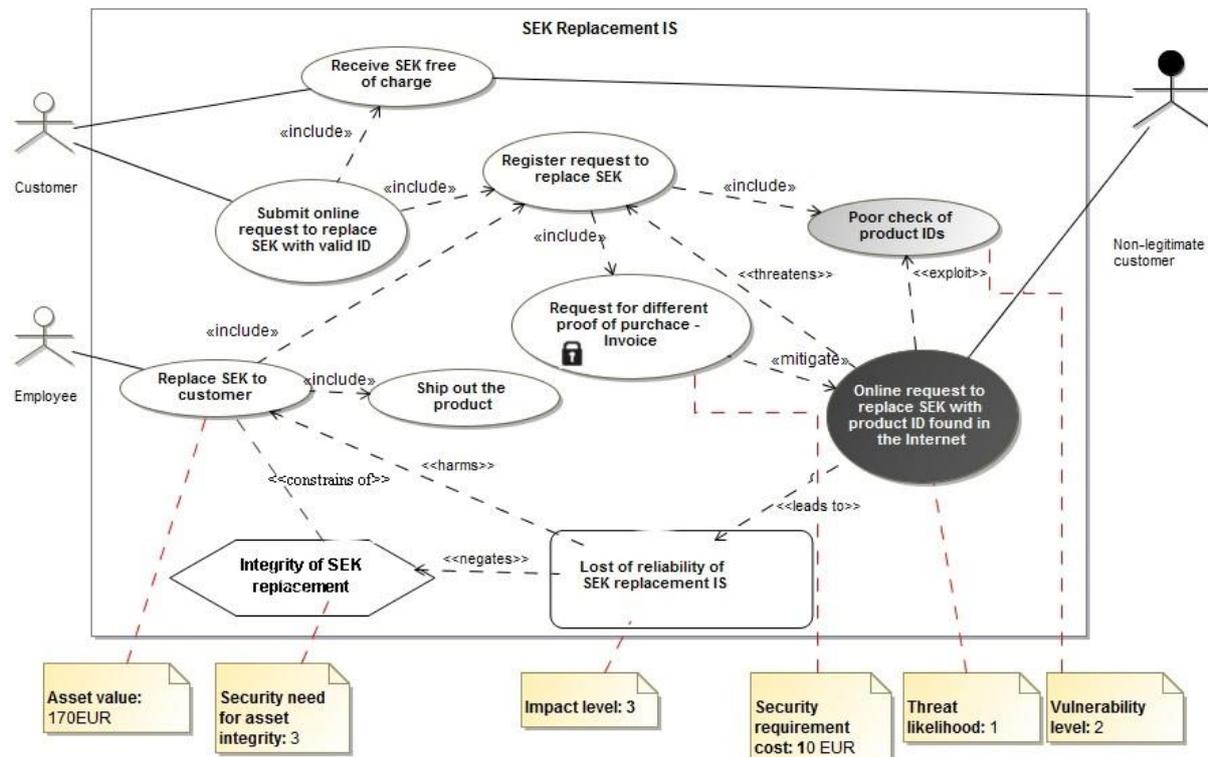


Figure 9. Introduction of metrics to misuse case diagram

With the help of Figure 9 we can now see and compare such risk measurement parameters as the asset value, security need, impact level, threat likelihood, vulnerability level and security requirement costs.

Next step is to introduce metrics within misuse case diagram and calculate the risk level, Risk Reduction Level (Figure 10), and Return on Security Investment (Figure 11). In order to calculate the total risk level (RL) we need to use following parameters: the vulnerability level, threat likelihood and impact level. For that we may use the risk treatment modeling diagram of misuse cases. Referring to the ISSRM model (Mayer, 2009), the formula for calculation of the risk level is:

$$RL = (Vulnerability\ level + Threat\ likelihood - 1) * Impact\ level$$

After the risk level was determined we have made a decision to avoid the risk and implement countermeasures (request for different proof of purchase) that will change values for the vulnerability level as well as threat likelihood. The vulnerability level(2) will be 0, meaning that security means are in place. Threat likelihood will be reduced to minimum, because it will not be possible for anyone to place the online replacement request only with the product ID. The threat likelihood(2) will be 1 as this is the minimum value. The formula for the calculation of risk level(2) is:

$$RL(2) = (Vulnerability\ level(2) + Threat\ likelihood(2) - 1) * Impact\ level(2)$$

Once we have calculated the risk level and the risk level(2) after the treatment, we can now determine the risk reduction level:

$$RRL = RL - RL(2)$$

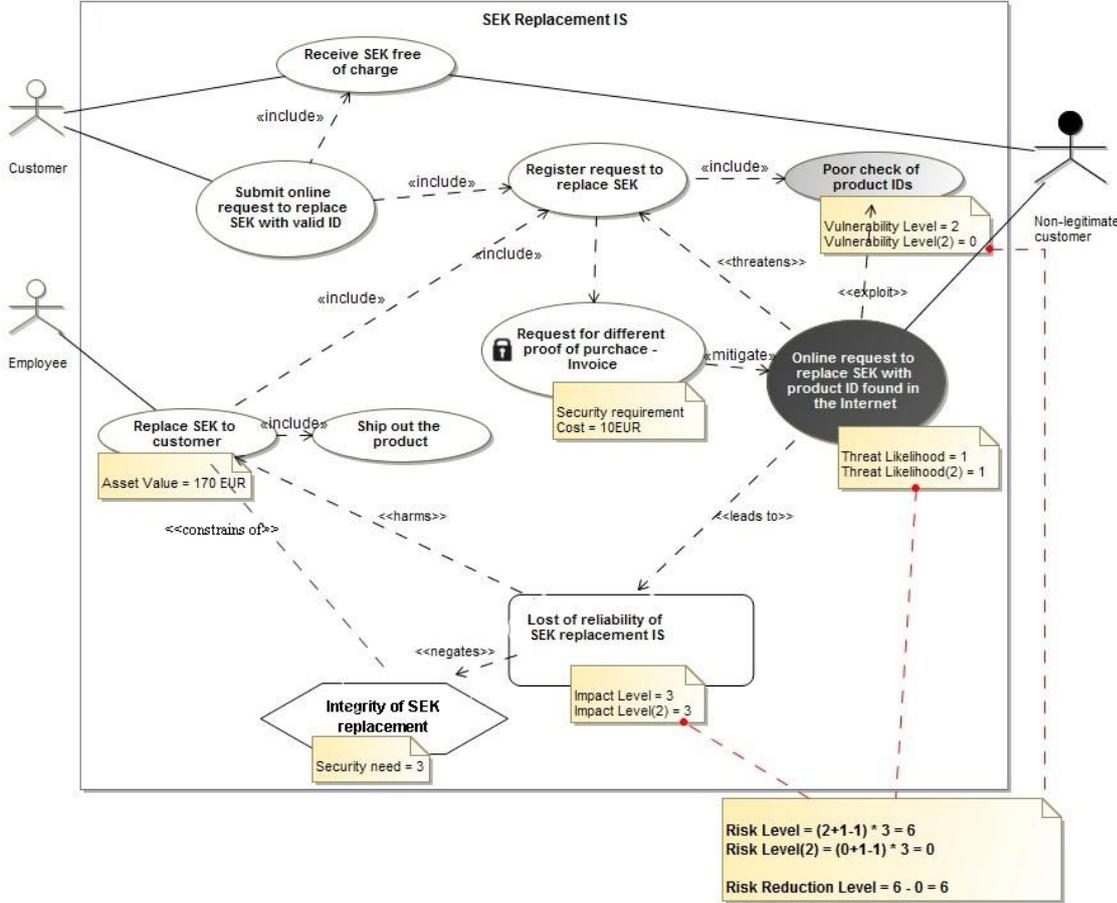


Figure 10. Risk Reduction Level Calculation - MUC

After we have defined the risk reduction level, we may calculate the ROSI, which in turn will give a valuable data for management about the benefit of the security control implementation. See Figure 11. For that we need such parameters as the security requirement cost, risk exposure (asset value) and the value of risk mitigation (RM). Risk mitigation is calculated by dividing the risk level to risk reduction level ( $RM = RR/RRL$ ). The formula for calculation of ROSI is as follows:

$$ROSI = [((Risk\ exposure * Risk\ mitigated) - Solution\ cost) / Solution\ cost] * 100\%$$

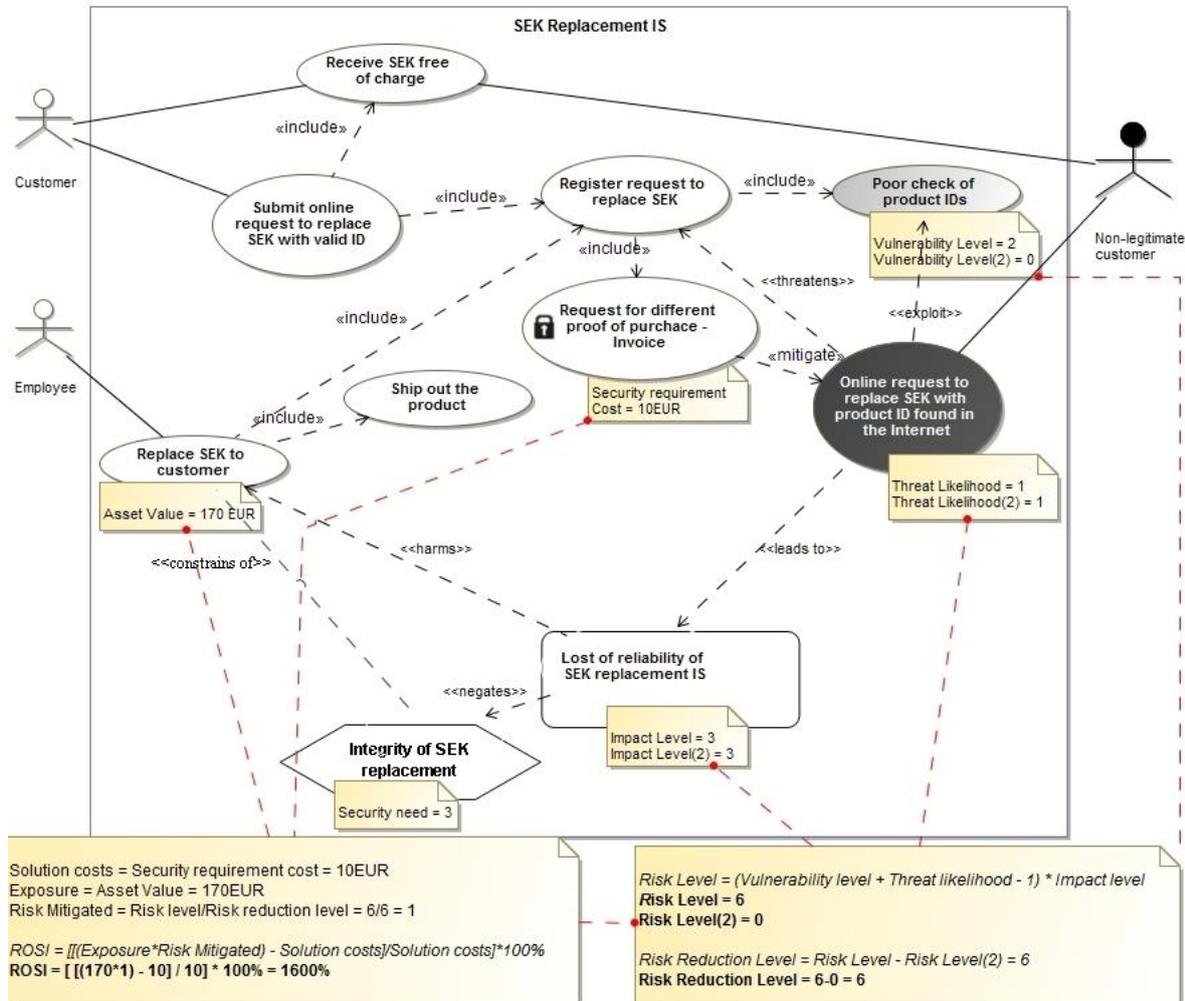


Figure 11. Calculation of ROSI - MUC

From Figure 11 we can see that the number of ROSI is 1600%, which is substantial. It is obvious, that the implementation of the security requirements will be profitable for the company. Moreover, it will avoid the risk, making the vulnerability level equal to '0'.

#### 4.2.2 SROMUC meta-model with metrics

In this section we will enrich SROMUC meta-model with metrics, proposed above and presented in misuse case diagrams. Following the pattern we enrich meta-model elements with values.

##### Business Asset Value

Looking at the misuse case diagram, Figure 11, we can see that the asset value is applied to the use case (replace SEK to customer). Figure 12 illustrates that an actor initiates the

communication to interact with one or more use cases. The illustrated use case represents the business asset, which is extended with value.

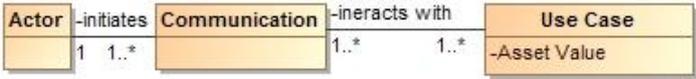


Figure 12. MUC - business asset concept

Vulnerability level

Figure 13 represents that the use case includes one or more vulnerabilities, which is extended with the measurement of vulnerability level. Since the use case is used to illustrate both business and information system assets, we do not have metrics for the use case element in this concept. The use case represents the IS asset here.



Figure 13. MUC - vulnerability concept

Security need

Security criterion, in Figure 14, which is a constraint of the use case (representing business asset value), was extended with security need measurement.

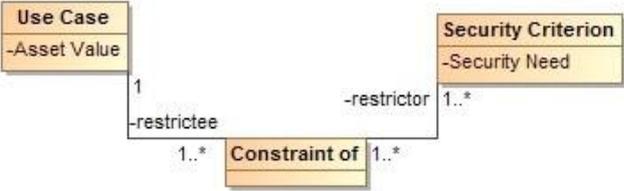


Figure 14. MUC - security criterion concept

Threat likelihood and event potentiality

In Figure 15 we can see that the use case (IS asset) includes one or more vulnerabilities that can be exploited by one or more misuse cases. A misuser initiates the communication to interact with the misuse case, thus it threatens one or more use cases (IS asset). The misuse case, representing a threat is extended with measurement threat likelihood.

Event is not represented as a separate construct in a meta-model, as it is a derived element. The event potentiality is calculated by summarizing the threat likelihood and vulnerability level and minus one.

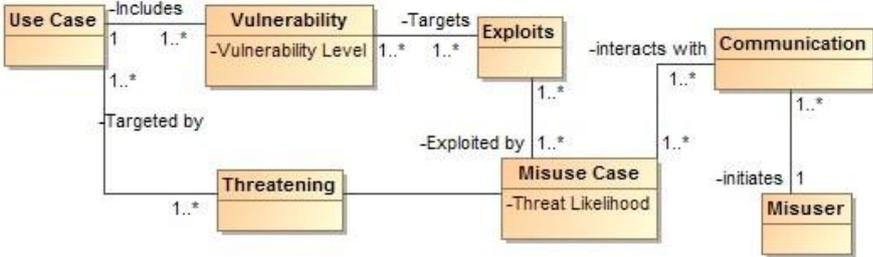


Figure 15. MC - threat and event concept

Impact level and risk level

A misuse case leads to one or more impacts. See Figure 16. An impact harms one or more use cases (business asset) by negating one or more security criteria, defined as constraint of that use case.

The concept in Figure 16 also illustrates the risk level. The level of risk is a derived value from the vulnerability level, threat likelihood and impact level.

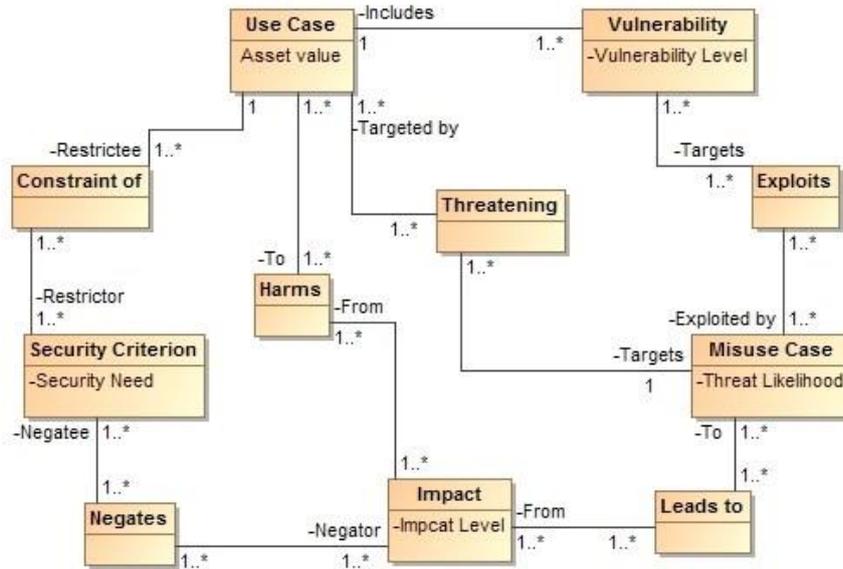


Figure 16. MUC - impact and risk concept

### Security requirement cost

The security use case in Figure 17 is a specialized use case that mitigates one or more misuse cases. It was extended with the value of security requirement cost.

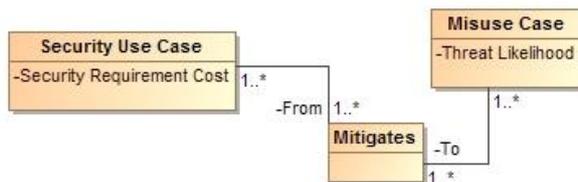


Figure 17. MUC - security requirement concept

The complete meta-model with introduced metrics is illustrated in Figure 18. The main elements of the meta-model in Figure 18 are an actor or misuser and use or misuse cases. An actor or misuser initiates the communication to interact with one or more use or misuse cases. Use or misuse case can include or extend the other use or misuse cases. The use case, which may include one or more vulnerabilities, can be exploited by one or more misuse cases is a specialization of use or misuse cases. A misuse case threatens one or more use cases and leads to one or more impacts, which, in turn, harm one or more use cases by negating one or more security criteria. A security use case is a specialization of use case that mitigates one or more misuse cases.

Every construct, illustrated in Figure 18, is a sub-class of a (Mis)Use Case constructs that are used to create (Mis)Use Case diagrams (see Figure 19).

With the help of misuse case diagrams we have introduced two derived metrics – ROSI and RRL.

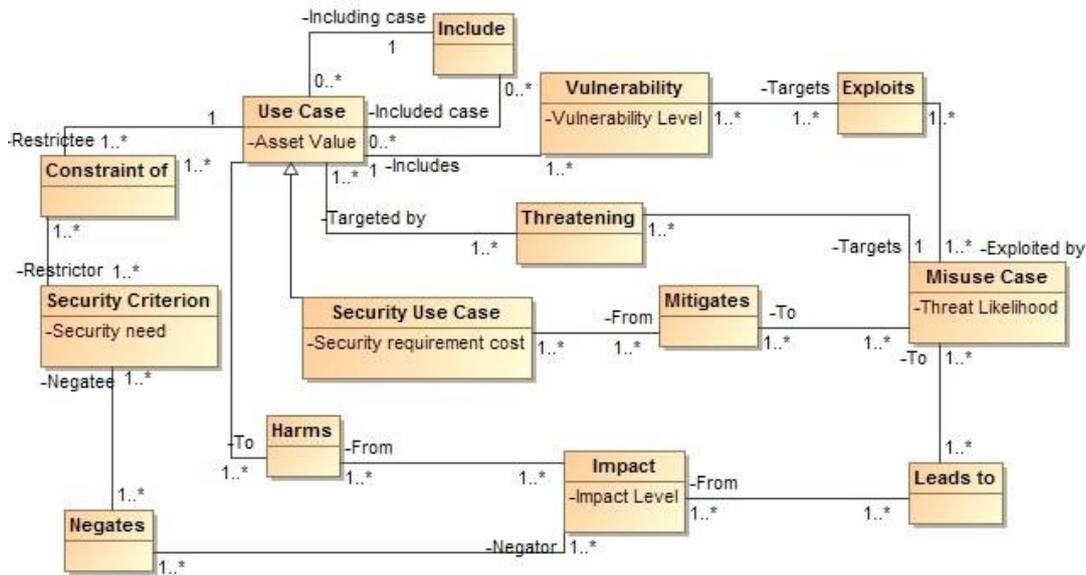


Figure 18. Complete SROMUC meta-model

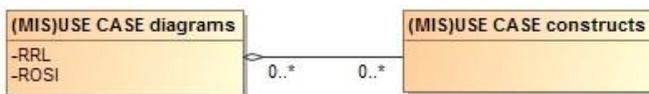


Figure 19. MUC – introduction of ROSI and RRL

### 4.3. Measurement model for BPMN

In this chapter we will introduce measurements for BPMN diagrams as well as for the meta-model, similarly to what we have done for misuse cases. Two derived metrics will be presented such as risk reduction level and return on security investment.

#### 4.3.1 Metrics within BPMN diagrams

Similar to what we have done to introduce metrics within misuse case diagrams, BPMN language was also extended with metrics. In Figure 21 we introduced the asset value, impact level, threat likelihood, security requirement cost and vulnerability level, using annotations. It turned out to be impossible to introduce all metrics in one diagram for BPMN. The security need had to be illustrated in a separate diagram of asset modeling. See Figure 20. The BPMN diagram allows illustrating either security constraint or impact at once. Nevertheless, it does not influence the further calculation of risk reduction level and return on security investments, since the metric for security need is not included in the calculation formula.

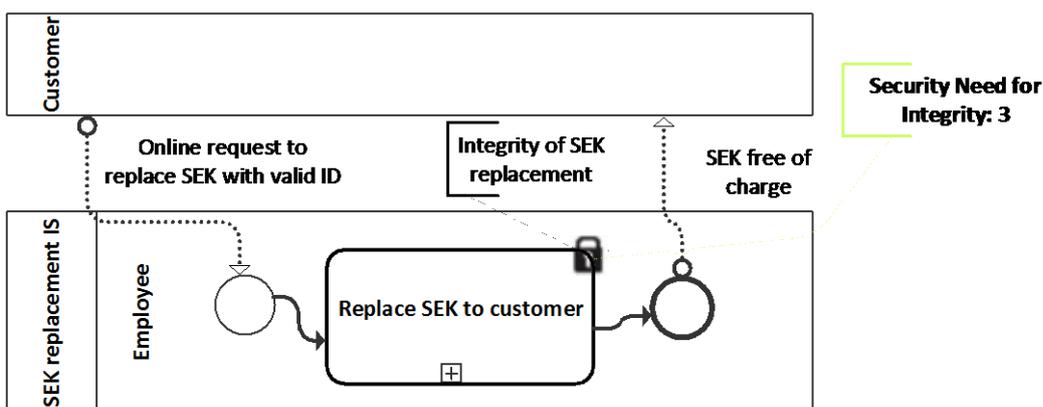


Figure 20. Introduction of security need metric to BPMN diagram

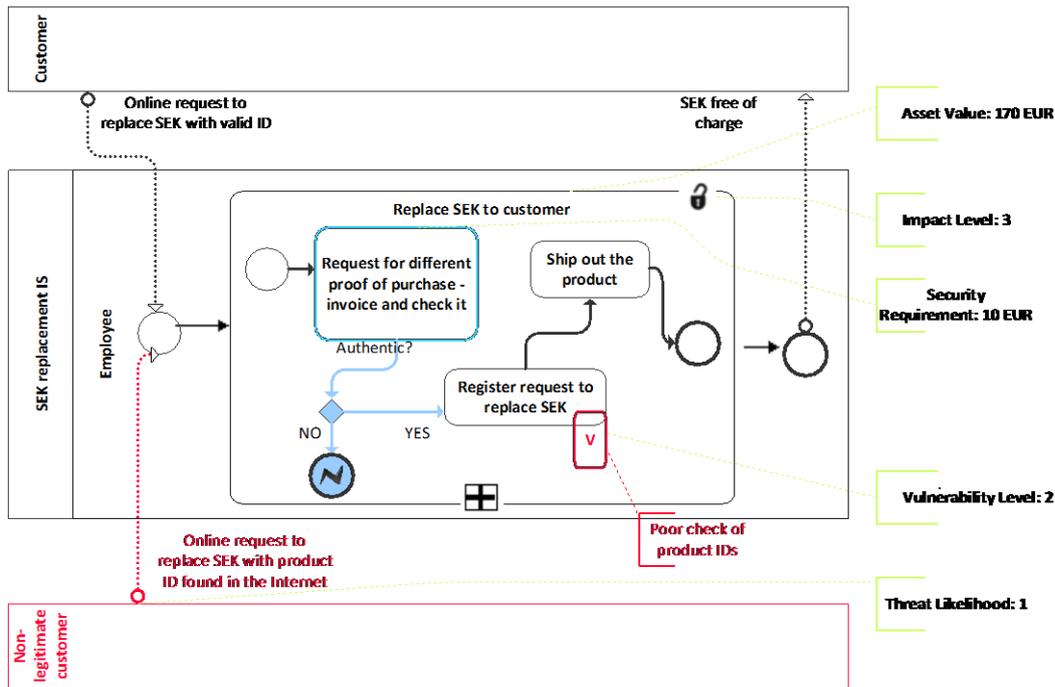


Figure 21. Introduction of metrics to BPMN diagram

Once we have introduced metrics into the BPMN diagram, we can now use them for further calculations. Following the formula presented below, we first calculate the risk reduction level (Figure 22). For that we first calculate the risk level before the security treatment and the risk level(2) after the security treatment in place. As we have those values, we can calculate the final risk reduction level:

$$RL = (Vulnerability\ level + Threat\ likelihood - 1) * Impact\ level$$

$$RL(2) = (Vulnerability\ level(2) + Threat\ likelihood(2) - 1) * Impact\ level(2)$$

$$RRL = RL - RL(2)$$

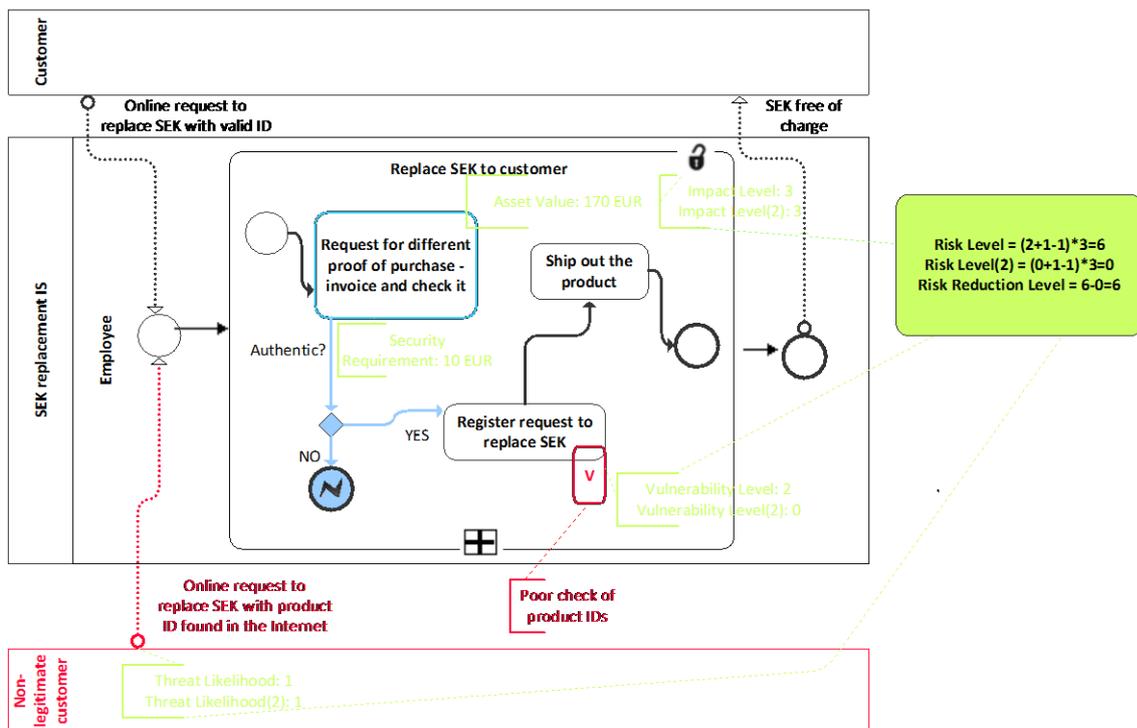


Figure 22. Risk Reduction Level calculation – BPMN

The second viewpoint on metrics is calculation of return on security investments. See Figure 23. This will give us clearer picture whether it is reasonable to mitigate the risk or not. The formula for ROSI calculation:

$$ROSI = [((Risk\ exposure * Risk\ mitigated) - Solution\ cost) / Solution\ cost] * 100\%$$

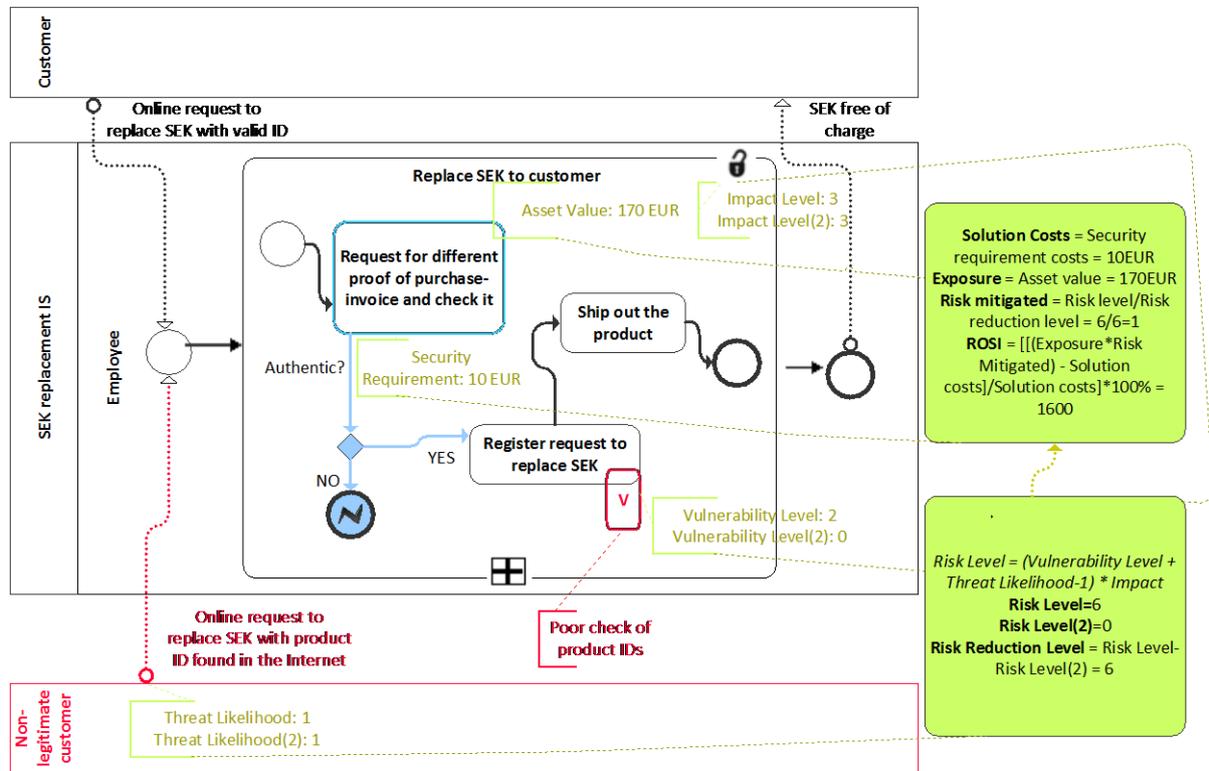


Figure 23. Calculation of ROSI - BPMN

### 4.3.2 Metrics within BPMN meta-model

The values for BPMN abstract syntax are presented step by step in separate elements, starting from the business asset value, vulnerability level, security need, threat likelihood, impact level, security requirement and finishing by the final meta-model, enriched with metrics.

#### Business asset value and security requirement cost

A business asset may be introduced by *data object* using *data association flow*, as proposed by Altuhova (2013). In addition, as illustrated in Figure 23, the business asset may also be introduced by the combination of such flow objects as *task*, *event* and *gateway*, using sequence flow. Therefore, flow object *task* is extended with the business asset value (Figure 24). Since the security requirement is illustrated also as a combination of flow objects, using the sequence flow (Figure 23), the security requirement cost is applied to the abstract construct *task* (Figure 24) together with the business asset value.

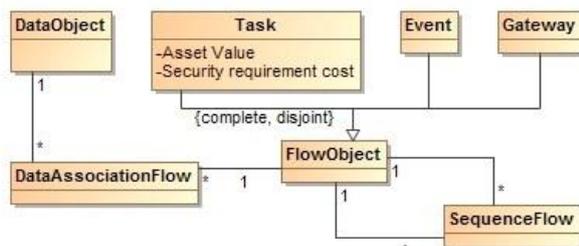


Figure 24. BPMN – business asset and security requirement cost concepts

Vulnerability level

*Vulnerability point* in Figure 25 is a property of *task* or *data store* (IS asset) and indicates the place of system weakness. The vulnerability point is extended with the measurement of vulnerability level. The vulnerability point is associated with annotation, in order to illustrate the actual weakness of a system.

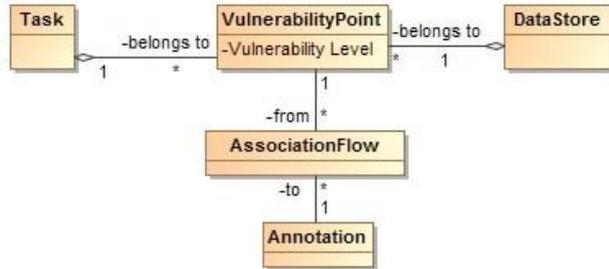


Figure 25. BPMN – vulnerability concept

Security need and impact level

The *lock* concept is defined to express the constraint of a valuable business with respect to the security objective – confidentiality, integrity and availability. The lock indicates whether the security criterion is maintained (*security objective*, see Figure 21) or negated (*impact*, see Figure 23). In case of indication of the security objective, *association flow* points from the *lock* to an *annotation*. The lock is a property of constructs that describe business assets. The impact is just a property of constructs that describe the business asset but does not have any association with an annotation.

In Figure 26 we introduce the security need (when security criterion is maintained) and in Figure 27 we see the impact level (when security criterion is negated).

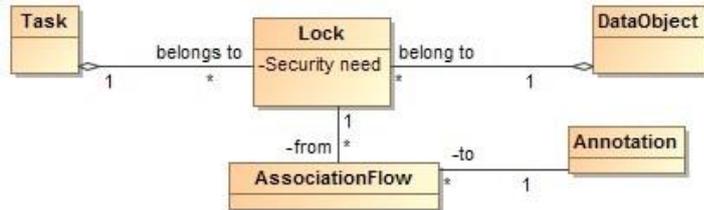


Figure 26. BPMN – security need concept

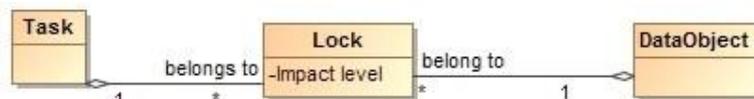


Figure 27. BPMN – impact concept

Threat likelihood

The combination of constructs for threat agent (pool and lane) and attack method (even, gateway and task) represents the threat. The threat likelihood is presented in an abstract construct of a *pool*. See Figure 28.

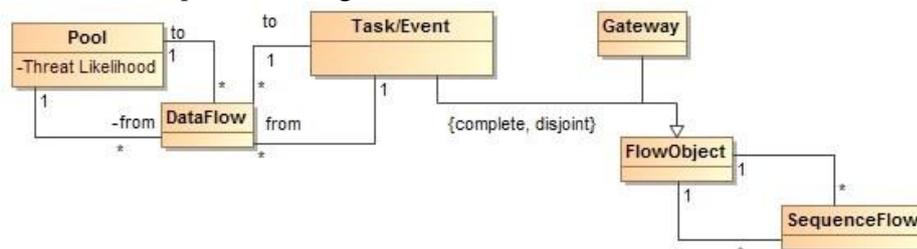


Figure 28. BPMN – threat concept



models of the security risk-aware modeling languages were aligned with proposed metrics as well. As a result of the applied metrics we were able to calculate the risk reduction level and return on security investments. Two developed models should provide information about the risk itself and the benefit from implementation of countermeasures in figures.

## **CHAPTER 5. Validation of Misuse Case and BPMN measurement models**

In this chapter we introduce the design of a survey conducted, describe the selection of participants, and present the goal of the questionnaire and its results. Moreover participants' feedback will be collected and the threat to validity presented.

### **5.1 Design**

The goal of our survey is to determine what the visibility of metrics in two proposed models is. In the composed questionnaire we examine which metrics and in which language (misuse cases or BPMN) it is easier to determine. First of all, we define the approach to validate two developed models and evaluate them. Secondly, we state which results we expect to receive. Then, we compose a questionnaire and collect answers from the respondents. Finally, we describe how the survey was conducted and what results we achieved.

### **5.2 Participant selection**

The participants, selected for validation of developed models were divided into two groups:

- People who know at least one modeling language, but are not aware of the security risk.
- People who do not know any modeling language, but are aware about the security risk.

Since our work was based on the example of the security risk taken from a working organization, we have approached 10 of its employees, who are aware of the security risk. Each person was provided with printed copies of RRL and ROSI calculation models for both languages (Figures 11 and 23). Everyone received a brief explanation about how the risk was modeled, using misuse case and BPMN languages. Next, employees were asked to answer the questionnaire (see Appendix A) independently.

In order to have a diverse data for the validity of the measurement model, we have also decided to selected software practitioners to participate in the survey. The diagrams with aligned metrics and the questionnaire were sent in attachment to the students, who are familiar with, at least, one modeling language.

### **5.3 Visibility questionnaire**

A questionnaire was prepared (Appendix A) to address questions in which out of two measurement models developed within misuse case (Figure 11) and BPMN (Figure 23) diagrams it is easier to identify expressions of proposed metrics. A feedback gathered from participants allowed us to compare those models.

In a survey document, firstly, a scenario of the security risk was briefly introduced. Secondly, the risk was modeled, using misuse case and BPMN diagrams together with proposed measurements. Finally, a questionnaire was composed, including 9 questions. By conducting a survey we were interested in the following aspects:

- Which metrics, introduced into the diagrams, and in which language it is easier to use them.
- Whether the two models can be understood by common users.
- Which model is preferable.

## 5.4 Results

Each participant was asked questions to give a feedback in which diagram it is easier to identify metrics, introduced to the modeling language of misuse cases and BPMN. The scale of answers gave options to answer whether it is “much easier”, “easier” or “somehow easier” to identify the metric in one diagram rather than in the other one. We have received 20 responses in total.

Table 7 gives us results of the survey, where the answers of 20 participants are presented. We can see that the choice of misuse cases and BPMN is equal. Nevertheless we identified that some of the metrics are of higher visibility in one of the languages and some are in other. For example risk level, RRL and ROSI are better visible in the misuse case diagram. These are all derived metrics. Impact level is also easier to identify using misuse cases. This may be explained by the fact that BPMN does not give any textual explanation for the impact. Values of the smaller components of the risk, such as vulnerability, threat and security requirement cost can be easier identified using BPMN language.

Table7. Total survey results

Questions	Participants	MUC	BPMN
Q1	20	11	9
Q2	20	8	12
Q3	20	8	12
Q4	20	15	5
Q5	20	12	8
Q6	20	8	12
Q7	20	14	6
Q8	20	17	3
Q9	20	10	10

Since we have composed our questionnaire using scale for evaluation of the visibility of values, we may look into the results of the survey in greater details. Table 8 presents the cross-cut results of the survey conducted among two groups of people: 1) Participants who are aware of the security risk scenario but who do not know any modeling language; 2) Participants who are familiar with various modeling languages but who are not aware of the security risk scenario. In the first column (Table 8) we present the questions. Then we divide the survey results according to the two groups of participants – *know the risk scenario* (we will later call Group R) and *know modeling languages* (we will later call Group L). For each group of participants we identify the total number of answered questionnaires. Finally, we illustrate how many participants have chosen misuse case or BPMN diagrams as an easier model to identify expressions of a particular value in a manner of a scale. For each answer the scale of “much easier”, “easier” and “somehow easier” was introduced. It means how easy it is to identify the metrics using one language in comparison to the other. The scale of “much easier” has the value of 3, “easier” has the value of 2 and “somehow easier” the value of 1. Based on these values and the number of participants that prefer one of the languages for identification of a particular risk metric, we came up with a formula that we use to weight the received answers:

$$MUC (Much\ easier * number\ of\ answers + easier * number\ of\ answers + somehow\ easier * number\ of\ answers) > < BPMN (Much\ easier * number\ of\ answers + easier * number\ of\ answers)$$

For the clarification we take an example of the first question. We have 1 answer in favor of MUC(much easier), 3 answers in favor of MUC(easier), 4 answers in favor of

BPMN(somewhat easier) and 2 answers in favor of BPMN(easier). Using our formula we can calculate the weight of the preferred modeling languages:

$$\text{MUC}(3*1+2*3+1*0) > \text{BPMN}(1*4+2*2+3*0)$$

The result we came up with is that MUC is a preferred modeling language in terms of the visibility of the asset value  $\{(MUC) 9 > (BPMN) 8\}$ . We apply the same formula for the rest questions and present the results in Table 8 in a separate row under each question.

Table 8. Cross-cut survey results

Q u e s t i o n s	Know the risk scenario						Know modeling languages							
	Number of participants	MUC			BPMN			Number of participants	MUC			BPMN		
		Much easier - 3	Easier - 2	Somehow Easier - 1	Somehow easier - 1	Easier - 2	Much easier - 3		Much easier - 3	Easier - 2	Somehow easier 1	Somehow easier - 1	Easier - 2	Much easier - 3
Q1	10	1	3		4	2		10	1	2	4		2	1
		$3*1+2*3+1*0 = 9$			$1*4+2*2+3*0 = 8$				$3*1+2*2+1*4 = 11$			$1*0+2*2+3*1 = 7$		
Q2	10	1	1	1	3	4		10	2	1	2	2	1	2
		$3*1+2*1+1*1 = 6$			$1*3+2*4+1*0 = 11$				$3*2+2*1+1*2 = 10$			$1*2+2*1+3*2 = 10$		
Q3	10		2	3	2	2	1	10	2		1	4	2	1
		$3*0+2*2+1*3 = 7$			$1*2+2*2+3*1 = 9$				$3*2+2*0+1*1 = 8$			$1*4+2*2+1*1 = 9$		
Q4	10	1	4	1	4			10	4	4	1	1		
		$3*1+2*4+1*1 = 12$			$1*4+2*0+3*0 = 4$				$3*4+2*4+1*1 = 21$			$1*1+2*0+3*0 = 1$		
Q5	10	3	1	2	2	1	1	10		1	5	2		2
		$3*3+2*1+2*2 = 15$			$1*2+2*1+3*1 = 7$				$3*0+2*1+1*5 = 7$			$1*2+2*0+3*2 = 8$		
Q6	10		3	1	2	4		10		1	3	3	1	2
		$3*0+2*3+1*1 = 7$			$1*2+2*4+3*0 = 10$				$3*0+2*1+1*3 = 5$			$1*3+2*1+3*2 = 11$		
Q7	10		3	4	2	1		10		2	5			3
		$3*0+2*3+1*4 = 10$			$1*2+2*1+3*0 = 4$				$3*0+2*2+1*5 = 9$			$1*0+2*0+3*3 = 9$		
Q8	10	1	6	2	1			10	1	1	6			2
		$3*1+2*6+1*2 = 17$			$1*1+2*0+3*0 = 1$				$3*1+2*1+1*6 = 11$			$1*0+2*0+3*2 = 6$		
Q9	10			4			6	10			6			4

*Q1. In which diagram – A or B – is it easier to identify the expression of the asset VALUE?* Group R (Table 8) considered in majority BPMN diagram to be clearer in representing the asset value. Nevertheless, the minority, who has chosen misuse cases, stated that it is either “easier” or “much easier” to identify the value. Whereas most of the participants who have chosen BPMN said that it is only “somehow easier”. But if we weight the received answers, using the formula presented above, we can see that misuse cases is still the preferred language for Group R (MUC9> BPMN8). Group L, on contrary, have stated in majority that the misuse case model is “somehow easier” to use while identifying asset value. Those participants, who have chosen to use BPMN, stated that it is either “easier” or “much easier” to use. Weighted answers also confirm that misuse cases is a preferred modeling language for the asset value identification.

**In general** (Table 7), misuse cases was identified as preferred security risk-oriented model for identification of the asset value.

*Q2. In which diagram – A or B – is it easier to identify the expression of the VULNERABILITY LEVEL?* Both Group R and L (Table 8) prefer BPMN in majority for identification of the vulnerability level. Weighted answers confirm these results.

**In general** (Table 7), BPMN was identified as preferred security risk-oriented model for identification of the vulnerability level.

*Q3. In which diagram – A or B – is it easier to identify the expression of the TREAT LIKELIHOOD?* Group R does not give any preferences for any model so the results are equal (Table 8). While weighted answers say that BPMN is a preferred language still. Group L prefers BPMN with vast majority for identification of the threat likelihood.

**In general** (Table 7), BPMN was identified as preferred security risk-oriented model for identification of the threat likelihood.

*Q4. In which diagram – A or B – is it easier to identify the expression of the IMPACT LEVEL?* This is one of the questions, where most of the participants from Group R and L consider misuse cases to be either “easier” or “much easier” model for identification of the impact level. In rest of the questions the scale “somehow easier” was chosen. All those participants, that preferred BPMN, said that it is only “somehow easier” to use the language. A clear advantage of misuse cases is visible also after the results were weighted (Table 8). Such preference may be explained by the fact that the impact construct is only expressed by an unlock image without any textual descriptions in BPMN.

**In general** (Table 7), misuse cases was identified as preferred security risk-oriented model for identification of the impact level.

*Q5. In which diagram – A or B – is it easier to identify expression of the RISK LEVEL?* Participants from Group R (Table 8) have chosen misuse case diagram with a slight preference as identification of a risk level. The weighted answers say that the preference of misuse cases is big. Group L has given the preference for the BPMN in both average and weighted answers.

**In general** (Table 7), misuse cases was identified as preferred security risk-oriented model for identification of the risk level.

*Q6. In which diagram – A or B – is it easier to identify the security requirement COST?* Group R (Table 8) preferred the misuse case diagram while Group L preferred the BPMN diagram. This may be explained by the fact, that in misuse cases the security requirement is visualized by the lock and therefore, clearly visible for participants who are not familiar with

modeling languages. Nevertheless after the answer was weighted it turned out that Group R still gave preference to BPMN.

**In general** (Table 7), BPMN is preferable for the identification of security requirement cost.

*Q7 and Q8. In which diagram – A or B – is it easier to identify the RRL (Q7) and ROSI (Q8)?*

The majority of participants from both Groups (Table 8) consider identification of RRL and ROSI to be easier while using the diagram of misuse cases. The interesting observation is, nevertheless, that some of them would still prefer using BPMN in general and have chosen this language to identify the rest of the values. Weighted answer gives the same result.

**In general** (Table 7), misuse cases is preferable for the identification of RRL and ROSI.

*Q9. If you need to use modeling notations to understand and to justify the security countermeasures, which language – misuse cases (A) or BPMN (B) – would you prefer?*

Group R (Table 8) prefer using misuse cases, while Group L prefer in majority BPMN.

**In general** (Table 7), there is an equal number of the participants who would prefer using misuse cases and BPMN.

The findings (Table 8) indicate that metrics of such constructs as the vulnerability, threat and security requirement can be easier identified, using BPMN graphical measurement model, whereas derived metrics, such as risk level, RRL, ROSI are better understood, using the misuse case graphical diagram.

The general feedback received from Group R was that both diagrams are quite hard to be read and require deep additional analysis and knowledge background. Some of the concepts were not fully understood and the answers to some questions were mainly intuitive (which concept is faster to find). Some also mentioned that misuse case diagram was easier to analyze in terms of metrics, whereas BPMN described the process itself clearer. The possible reason for that is that both languages represent different perspectives of the information system, while misuse cases represent the static perspective (relationship between different actors are described more clearly, though). BPMN represents both the static and dynamic perspectives. Therefore, misuse cases do not show in which order the activities are executed while in BPMN it is very easy to see the order of their execution.

The general feedback received from Group L was that the graphical description of the security risk, using both modeling languages, is an improvement, but is not intuitive and needs some further improvements in visual alignments.

Having weighted the received answers, we may assess how well we did our work in introducing the metrics into the modeling languages. For that we compare the maximum score that may be received for identification of the particular metric and compare it to the score we received from participants. The maximum score for the identification of the metric would be 30 (*much easier\*maximum number of answers = 3\*10 = 30*). For the identification of the asset value we have the score of 9 from participants. It means that the metric is not that visible, making up only 30% (*score received/maximum possible score\*100% = 9/30\*100% = 30%*). See Table 9. The Q9 is not included into the table since the answer does not include any evaluation scale.

Table 9. Evaluation of visibility of proposed metrics

Question	Description	Know the risk		Know the language	
		MUC	BPMN	MUC	BPMN
Q1	Weighted answer	9	8	11	7
	Visibility in %	30%	26%	36%	23%
Q2	Weighted answer	6	11	10	10
	Visibility in %	20%	36%	33%	33%
Q3	Weighted answer	7	9	8	9
	Visibility in %	23%	30%	26%	30%
Q4	Weighted answer	12	4	21	1
	Visibility in %	40%	13%	70%	3%
Q5	Weighted answer	15	7	7	8
	Visibility in %	50%	23%	23%	26%
Q6	Weighted answer	7	10	5	11
	Visibility in %	23%	33%	16%	36%
Q7	Weighted answer	10	4	9	9
	Visibility in %	33%	13%	30%	30%
Q8	Weighted answer	17	1	11	6
	Visibility in %	56%	3%	36%	20%

Table 9 indicates that the average score we received for the introduced metrics is ca. 30%, which means that the work in general still needs an improvement. The visibility of such metrics as ROSI and impact level in BPMN is extremely bad, while the visibility of ROSI and impact level in MUC is pretty good. Still, the approach to see how well we did the visualization of metrics (Table 9) has one major limitation. It may indicate not only whether the particular metric itself is clearly visible, but just how well it is visible in comparison to two languages. For instance, if a participant chooses the visibility of the asset value in MUC as “somehow easier”, it may mean that either it is not clearly visible in general or it is just slightly better visible comparing to BPMN.

### 5.3 Participants feedback

Along with the answers to our questionnaire we have received a feedback from some of the participants. We would like to present some comments, first of all, from people who know the risk scenario:

*“The problem is that both diagrams are quite hard to read and require additional analysis. A more simplistic approach would be recommended.”*

*“I am sorry but it seems to be very complicated. So I would like to give up the participation.”*

*“Since I did not know any modeling language before, it took me quite a lot of time to study the questionnaire. As an amateur I would say that it does not make a lot of difference as to where it is easier to use metrics.”*

As we can see from the comments above and the ones received personally, in general, people found the questionnaire itself together with the models quite complicated. While answering the questions, general concepts of the risk were hardly understood by participants. They often evaluated just graphical representations of the models and found places where it was easier to identify requested metrics. This is exactly what we were aiming at to validate.

There were also some comments from participants who are aware of modeling languages:

*“I think both are an improvement with regard to information provided but when I first sit down and look at either example they are not intuitive.”*

*“I believe reader can easily find out the elements that you have mentioned in the survey. The reason I prefer BPMN diagrams is that the elements were described more systematically.”*

*“Most of the answers are actually at the same level in both BPMN and MISUSE CASE diagrams. Maybe it would be wise to add the option of “Same” or something similar to that.”*  
*“It was really hard to answer questions about risk level, RRL, solution costs, ROSI as they are equally easy to outline from both models.”*

According to the feedback collected, we may conclude that it was quite easy to identify metrics in the misuse case and BPMN diagrams for participants who know modeling languages. But this is applicable only for our specific risk scenario. In case of a larger diagram, the concepts may be very hard to be followed. This will be discussed in greater details in the next chapter, in the limitations section.

#### **5.4 Threat to validity**

The ideal approach to measure the visibility of models cannot be found since there are always present some limitations. We have identified the following limitations to our approach:

- The participants may have had little real ambition to assess the two measurement models. Therefore, they may superficially have gone through the graphical description of the security risk. Thus, the answers from them may be partially based on a random choice.
- The choice may have been biased in case a participant knew one of the proposed languages and did not know the other one. If, for example, a participant knew MUC and did not know the BPMN it is obvious that it was easier for him to use the representation of metrics within MUC diagram.
- A rather small amount of participants may present a minor threat to validity.
- The risk example is a small one, in case of a more complex risk scenario the introduced metrics may not be possible to apply to the modeling languages.

#### **5.5 Summary**

In order to compare in which measurement model it is easier to identify proposed metrics, we have developed a questionnaire. The survey was conducted among two groups of people 1) who know the modeling languages and do not know the security risk scenario and 2) who do not know modeling languages but know the scenario of the security risk in detail. All in all, we collected and summarized the results of the survey and identified threats to validity.

## CHAPTER 6. Conclusion and Future Work

In this chapter we will conclude what has been done in the paper, state the limitations for the work and identify paths for the future research.

### 6.1 Conclusion

The goal of this paper was to visualize a single risk with metrics in two modeling languages: the misuse cases and BPMN and then evaluate in which model the visualization of metrics is clearer. In this paper we have introduced metrics to the security-aware misuse case and BPMN diagrams. Then we have conducted a survey in order to evaluate which expression of a metric and in which modeling language is easier to identify. This allowed us to answer our two research questions.

*RQ1: How to introduce the security risk measurement into the Misuse Cases and BPMN diagrams?* In order to introduce the security risk measurement, we have, first of all, studied the literature about various security risk management standards and approaches. We have also read papers about modeling languages and their alignment with such a security risk method as the ISSRM domain model. We have found out that the authors of the ISSRM model have introduced metrics, which served as a background for the current paper. Then we have identified one risk scenario from a working organization and illustrated it, using the misuse cases and BPMN. Finally, two graphical descriptions of the risk were enriched with metrics for the asset value, security need, impact level, security requirement cost, vulnerability level and threat likelihood. Having those parameters, we were able to introduce the calculations of RRL and ROSI for both measurement models.

*RQ2: Which modeling language extended with metrics (misuse cases or BPMN) is of higher understandability for its users?* The second part of our contribution was to conduct a survey in order to analyze which proposed metrics and in which modeling language it is easier to use them. This led us to results, that the BPMN language is preferred for identification of values for such constructs as the vulnerability, threat and security requirement. While misuse cases is much more preferred for identification of the risk level, RRL and ROSI.

### 6.2 Limitations

As any other research work, this paper has some limitations. First of all, the identified problem is rather a small one and the suggested model cannot be extended to more complex and bigger problems. However, the problem identified is a real one and the visualization of the risk with metrics was presented to the management of a company. Secondly, the two models are focused on comprehensibility; hence the correctness remains a question. While answering a survey participants may have been either biased by one of the language or just misunderstood the models at all. Thirdly, the paper does not provide any technical solutions as how to measure the risk automatically, due to the lack of IT background of the author. Finally, two proposed measurement models do not provide any measurement approaches to compare which security requirements are wiser to implement. The reason for that is that the risk scenario considered only one possible security requirement.

### 6.3 Future work

We have illustrated a rather small and simple risk in this paper. Therefore, the alignment of metrics for more complex risks may be the idea for a future research. Also the scope of this work is limited to the graphical representation of the introduced metrics in two modeling

languages. Alignment of a textual template for misuse cases can be treated as a future task as well. Since our models illustrate only one security requirement, we did not work on the prioritization of possible requirements. The way, how to measure and decide which security requirements are wiser to take into consideration, will remain a subject for further research. Next, we have provided the visualization of the risk together with the metrics for the misuse cases and BPMN. In future a tool may be developed in order to facilitate the modeling of a risk together with its metrics and calculations of RRL and ROSI. Finally, other modeling languages may also be aligned with metrics.

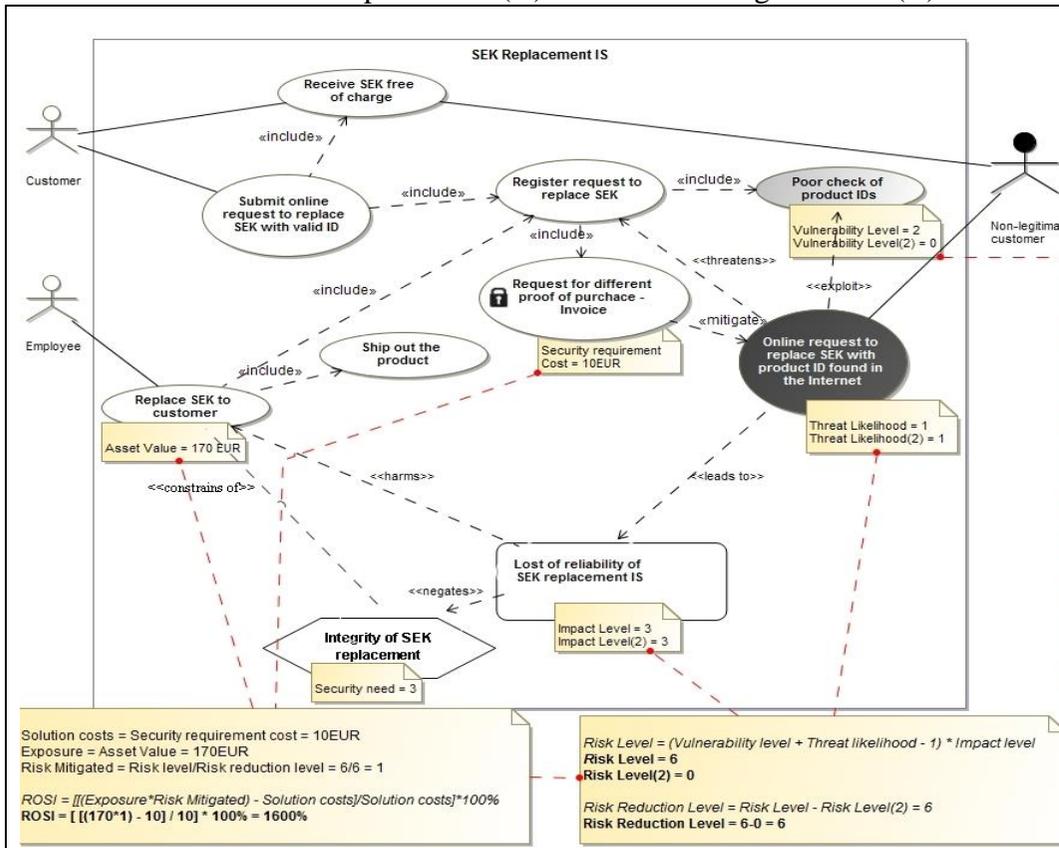
The same way as we have introduced metrics into the diagrams of misuse cases and BPMN, we would like to discuss how these metrics can be introduced into other modeling languages. As an example we will take Mal-Activity, which is abbreviated as MAD. The language describes the procedural logic, business process and work flow (Soomro, 2012). Since Mal-Activity is already aligned with the ISSRM domain model (Chowdhury, 2012), it is easier to identify such constructs as business and IS asset, vulnerability, security criterion, threat, impact and security requirements in the graphical diagram. Once these constructs are identified, we can apply metrics to all of them. Finally, calculations of risk level, RRL and ROSI are possible. These calculations may be visualized in the legend of MAD.

## References

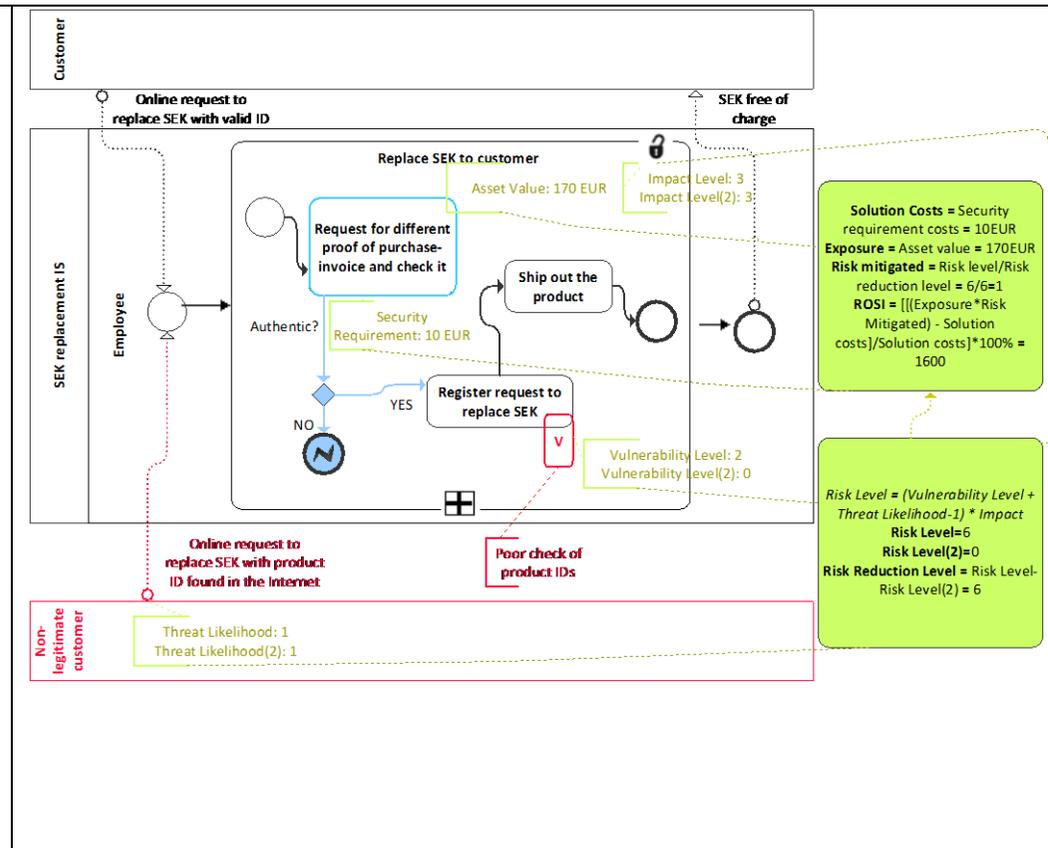
1. Alberts C. and Dorofee A., *Managing Information Security Risks, the OCTAVE Approach*, Pearson Education, Inc, 2003
2. Altuhhova O., *An Extension of Business Process Model and Notation for Security Risk Management*, Master's thesis, Tartu, 2013
3. Altuhhova O., Matulevičius R. and Ahmed N., *An Extension of Business Process Model and Notation for Security Risk Management*, Estonia, 2012  
[https://courses.cs.ut.ee/MTAT.03.246/2013\\_spring/uploads/Main/bpmn.pdf](https://courses.cs.ut.ee/MTAT.03.246/2013_spring/uploads/Main/bpmn.pdf)
4. Chowdhury M. J. M., *Towards Security Risk-oriented Mal Activity Diagrams*, IJoCA, 2012
5. Dhillon G. and Backhouse J., *Information System Security Management in the New Millennium*, Communications of the ACM, 2000
6. ISO/IEC 27001. *Information technology-Security techniques-Information security management systems-Requirements*, International Organization for Standardization, Geneva, 2005
7. ISO/IEC 27005. *Information technology-Security techniques-Information security risk management*, International Organization for Standardization, Geneva, 2008
8. Jenkins B. D., *Security Risk Analysis and Management Countermeasures*, Inc., 1998,  
[http://www.nr.no/~abie/RA\\_by\\_Jenkins.pdf](http://www.nr.no/~abie/RA_by_Jenkins.pdf)
9. Matulevičius R., *Model Comprehension and Stakeholder Appropriateness of Security Risk-oriented Modelling Languages*, accepted at EMMSAD, 2014
10. Matulevičius R., Mayer N., Heymans P., *Alignment of Misuse Cases with Security Risk Management*, IEEE Computer Society, 2008
11. Mayer N., *Model - Based Management of Information System Security Risk*, Belgium, 2009  
[http://www.nmayer.eu/publis/Thesis\\_Mayer\\_2.0.pdf](http://www.nmayer.eu/publis/Thesis_Mayer_2.0.pdf)
12. Neubauer T., *A Comparison of Security Safeguard Selection Methods*, Austria, 2009  
[http://publik.tuwien.ac.at/files/PubDat\\_198401.pdf](http://publik.tuwien.ac.at/files/PubDat_198401.pdf)
13. NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, Gaithersburg, 2012  
[http://www.nist.gov/customcf/ge\\_pdf.cfm?pub\\_id=912091](http://www.nist.gov/customcf/ge_pdf.cfm?pub_id=912091)
14. Owen M. and Raj J., *BPMN and Business Process Management*, Popkin Software, 2003
15. Pantazis, *CRAMM (CCTA Risk Analysis Management & Methodology)*, 2011  
<http://itsecurityoffice.blogspot.com/2011/09/cramm-ccta-risk-analysis-management.html>
16. Shimonski R. J., *Risk Assessment and Threat Identification*, 2002  
[http://www.windowsecurity.com/articles-tutorials/misc\\_network\\_security/Risk\\_Assessment\\_and\\_Threat\\_Identification.html](http://www.windowsecurity.com/articles-tutorials/misc_network_security/Risk_Assessment_and_Threat_Identification.html)
17. Sindre G., Opdahl A., *Eliciting security requirements with misuse cases*, London, 2002
18. Soldal Lund M., Solhaug B., Stolen K., *Model-Driven Risk Analysis, The CORAS Approach*, Norway, 2011  
[https://courses.cs.ut.ee/MTAT.03.246/2013\\_spring/uploads/Main/bpmn.pdf](https://courses.cs.ut.ee/MTAT.03.246/2013_spring/uploads/Main/bpmn.pdf)
19. Soomro I., *Alignment of Misuse Cases to ISSRM*, Master's thesis, Tartu, 2012
20. Soomro I. and Ahmed N., *Towards Security Risk-oriented Misuse Cases*, Estonia, 2013
21. Talbot J., Jakeman M., *Security Risk Management Body of Knowledge*, New Jersey, 2009  
[http://www.omg.org/bpmn/Documents/6AD5D16960.BPMN\\_and\\_BPM.pdf](http://www.omg.org/bpmn/Documents/6AD5D16960.BPMN_and_BPM.pdf)

# Appendix A. Survey

**Scenario:** A *customer* (user of a SEK replacement system) seeks to replace broken Sculpt Ergonomic Keyboard (SEK) free of charge under the warranty rules. The customer submits the online request to replace the SEK using valid product ID. The *request to replace SEK* is registered in a *system* (IS asset) by the *employee* (user of a SEK replacement system). The employee seeks to *replace SEK to customer* (business asset) with the security criterion of *integrity of SEK replacement* imposed on it. A *non-legitimate customer* (misuser) can also place an *online request to replace SEK free of charge with a product ID found in the Internet* (threat). Such action leads to the *loss of reliability of the SEK replacement system* (impact). Such risk is possible because there is a weakness in a system - *poor check of product IDs* (vulnerability). In order to avoid such risk countermeasure to *request for a different proof of purchase*, which is not easy to falsify (security requirement) is implemented. This situation is expressed in (A) Misuse case diagrams and (B) BPMN diagrams below.



A: Misuse case diagram



B: BPMN diagram

<p style="text-align: center;"><b>A.</b> <b>Misuse case diagram</b></p>	<p style="text-align: center;"><b>B.</b> <b>BPMN diagram</b></p>
<p><b>Q1.</b> A process <i>Replace SEK to customer</i> is an important (business) asset in this scenario. It has <b>value</b>, which equals to 170 euro. <b>In which diagram – A or B – is it easier to identify the expression of the asset VALUE?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>
<p><b>Q2.</b> In this case, system vulnerability is <i>Poor check of product IDs</i>. The <b>vulnerability level</b> is <b>2</b> before treatment and <b>0</b> after security treatment. <b>In which diagram – A or B – is it easier to identify the expression of the VULNERABILITY LEVEL?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>
<p><b>Q3.</b> A process <i>Online request to replace SEK with product ID found in the Internet</i> is identified as the attack method threat in this scenario. This attack method is a part of the security threat. In our case the <b>threat likelihood</b> has a value of 1 before and after security treatment. <b>In which diagram – A or B – is it easier to identify the expression of the TREAT LIKELIHOOD?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>
<p><b>Q4.</b> <i>Lost of reliability of SEK replacement IS</i> is a part of the impact in this scenario. <b>Impact level</b> has a value of 3 before and after security treatment. <b>In which diagram – A or B – is it easier to identify the expression of the IMPACT LEVEL?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>

<p style="text-align: center;"><b>A.</b> <b>Misuse case diagram</b></p>	<p style="text-align: center;"><b>B.</b> <b>BPMN diagram</b></p>
<p><b>Q5.</b> Risk level is calculated taking into account the <i>threat likelihood, vulnerability level, and impact level</i>. In our scenario initial <b>Risk level</b> has a value of <b>6</b> and <b>risk level</b> after security treatment (risk avoidance) equals to <b>0</b>. <b>In which diagram – A or B – is it easier to identify the both expressions of the RISK LEVEL?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>
<p><b>Q6.</b> A process <i>Request for different proof of purchase - invoice</i> is identified as a possible security requirement. It has a <b>cost</b> which equals to <b>10</b> euro. <b>In which diagram – A or B – is it easier to identify the security requirement COST?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>
<p><b>Q7.</b> <i>Risk Reduction Level</i> is a derived metric, which gives quantitative information about the benefit of countermeasure. In our scenario it equals to <b>6</b>. <b>In which diagram – A or B – is it easier to identify the RISK REDUCTION LEVEL?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>
<p><b>Q8.</b> <b>Return on Security Investment (ROSI)</b> is a derived metric, which helps the security specialist to make a decision if an investment into a particular security solution is justifiable. In our scenario ROSI appears to be <b>1600%</b>. <b>In which diagram – A or B – is it easier to identify the calculation of ROSI?</b></p>	
<p><input type="checkbox"/> Much easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Somehow easier</p>	<p><input type="checkbox"/> Somehow easier      <input type="checkbox"/> Easier      <input type="checkbox"/> Much easier</p>

**Q9.** If you would need to use modeling notations to understand and to justify the security countermeasures, which language – **misuse cases** (A) or **BPMN** (B) – would you prefer?

MISUSE CASE  
diagrams

BPMN  
diagrams

If you have any comments or suggestions, please write them in the field below:

--

**THANK YOU!**

## **Appendix B. License**

Non-exclusive license to reproduce thesis and make thesis public.

**Anna Preobrazenskaja** (date of birth: 03.01.1987),

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

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

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

**Development of Security Risk Measurement Model within Misuse Cases and BPMN,**

Supervised by Raimundas Matulevičius,

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

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

Tartu, **26.05.2014**