Combining Information Security Risk Management and Probabilistic Risk Assessment

Kärt Padur and Raimundas Matulevičius[0000−0002−1829−4794]

Institute of Computer Science, University of Tartu,
J. Liivi 2, 50409 Tartu, Estonia
kart.padur@ttu.ee, rma@ut.ee

Abstract. Information security risk assessment is an important activity, which helps to explain risk exposure and to asset security need. However, on one hand, a lot of methods use the subjective measurements, which does not allow capturing accurate estimates. On other hand, application of the quantitative methods requires time and efforts. In order to mitigate their limitations, we discuss how to do some to combine both qualitative and quantitative methods for the security risk management. We illustrate this combination in the running example.

Keywords: Information Security Risk Assessment, ISSRM, Bayesian Network Based Attack Graphs.

1 Introduction

Organisations want to pursue their business ambitions while operating in a secure environment. Hence, the information security risks have to be assessed. Today, organisations use qualitative security risk management methods, which take value judgements as input to the analysis [1]. It saves time, effort, and expenses [26]. However, these methods rely on subjective judgment, focus on concepts and principles, and do not provide monetary values [10]. Alternatively, the use of quantitative probabilistic risk assessment methods, which use measured data as input to limit subjectivity of the analysis, can be considered. However, the process of gathering data and managing it requires more time and effort [1]. In this paper we suggest a hybrid approach where the qualitative and quantitative method are combined together. Such a combination allows one to use the subjective and measured data [26].

The structure of the paper is the following: In Section 2 we present the theoretical background. In Section 3 we present a combination of the qualitative and quantitative methods and in Section 4 we illustrate their application in a running example. Section 5 concludes the paper and present some future work.

2 Theory

There is a number of information security risk management standards and frameworks available for organisations to use, e.g. ISO/IEC 27005 [12], NIST 800-30

Copyright © 2019 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

CEUR-WS.org/Vol-2443/paper02.pdf

[19], FAIR approach [9], OCTAVE Allegro framework [2], COSO framework [4]. There is no specific information security risk management standard or framework for financial institutions. Two methods – Information System Security Risk Management (ISSRM) [5] [14] and Bayesian Network Based Attack Graph (BNBAG) [10] [18] – are used to assess the information security risk. In this paper ISSRM is selected because it supports a security risk management and BNBAG – because it is a probabilistic risk assessment method.

2.1 Information Systems Security Risk Management

The ISSRM method [5] [14] helps to ex-plain assets that are valuable and need protection against the certain security risks and security countermeasures that need to be selected to mitigate these risks. It consists of a domain model, metrics and process for managing the security risks.

Domain model. The domain model for ISSRM, presented in Fig. reffig1, has three groups of concepts: asset-related concepts, risk-related concepts, and risk-treatment related concepts. *Asset-related concepts* emphasize which assets are important to be protected according to the security needs of the system. *Assets* are either *business assets* or *information system* (*IS*) *assets*. A business asset is any information, process or skill that is necessary for an organisation. It is characterised by the *security criterion* of confidentiality, availability, or integrity. Information system assets are valuable parts of IS as they provide support for business assets. The second group is *risk-related concepts* which illustrate risk and its components. *Risk* is described as a *threat* that could exploit one or more *vulnerabilities*, leading to an *impact* that harms assets and negates the security criterion. A threat is a combination of a *threat agent* and *attack method*. *Risk treatment-related con-cepts* describe how to treat risk based on the knowledge of existing *controls* that implement *security requirements* which mitigate *risk*. Risk treatment is the decision whether to avoid, reduce, transfer or retain the risk. Risk treatment-related concepts are not a part of the scope of this paper.

Metrics. ISSRM method [5] [14] offers metrics to calculate risk. The *value* metric describes the value of a business asset considering the potential impact if the business asset is either disclosed, modi-fied or disrupted. The *security need* metric expresses the importance of the security criterion with respect to the business asset. The *likelihood* metric describes the likelihood of an attack considering the adversary's motivation and attack method sophistication. *Vulnerability level* metric describes the prevalence of the vulnerability and the likelihood of exploit. *Potentiality* is calculated us-ing the likelihood and vulnerability level metrics. *Impact level* metric is the maximum value that is assigned to the security need metric. *Risk level* metric is calculated as the product of *potentiality* and *impact level*. These five metrics describe risk-related concepts. In risk treatment-related concepts, risk treatment and security requirements are estimated using *risk reduction* and *cost*. Controls are estimated in terms of *cost*.

Process. The process of ISSRM [5] [14] introduces the activities to conduct information security risk management. The pro-cess begins with understanding the *context* where the organisation is operating and *identifying* its *business* and

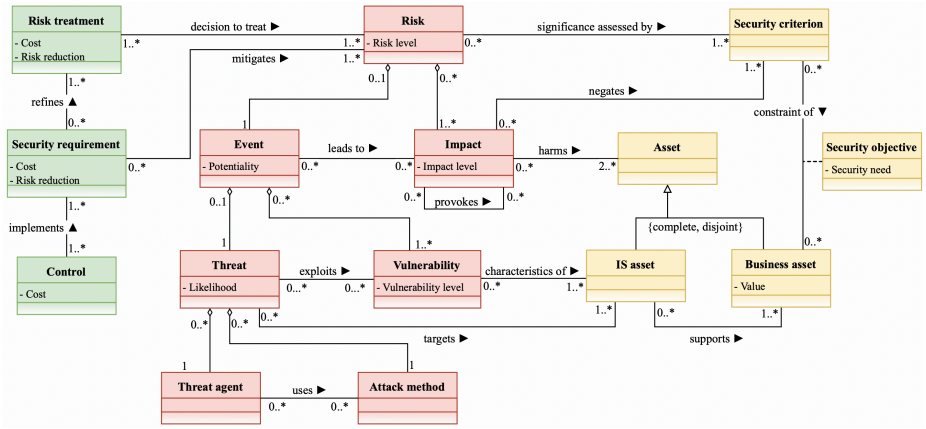

Fig. 1. ISSRM domain model (adapted from [5] [14])

IS assets. Next, the *security objectives* are determined in terms of confidentiality, integrity, and availability based on the level of protection needed for the assets. Then the *risk* is *analysed* and *assessed*. After these activities, it is decided whether the assessment is satisfying or not. These previous steps can be iterated in case of unsatisfying results. The following step is about *risk treatment* whether to avoid, reduce, transfer, or accept the risk. Then *security requirements* are to be defined to state the needed security conditions to achieve the desired level of security based on identified risks. If the treatment has been unsatisfying, then the whole process can be started from the beginning or from risk treatment step. The last step is about *selecting* and *implementing controls* based on security requirements.

2.2 Bayesian Network Based Attack Graphs

BNBAG method [10] [18] is a probabilistic risk assessment method which uses Bayesian Networks (BN) to model and analyse attack graphs to assess risk. It is based on Bayesian probability theorem which pro-vides a version to compute conditional probabilities.

Bayesian Probability Theory. Bayesian probabilistic reasoning starts with a hypothesis, H, for which the probability of hypothesis P(H) is called the prior belief about H. Evidence, E, is used to revise the belief about H using the likelihood of evidence, P(H|E). The posterior belief about H in the light of evidence is calculated [10]. Bayes' theorem states that the probability of the hypothesis given the evidence is equal to the probability of the evidence given the hypothesis times the probability of hypothesis divided by the probability of evidence [11]. There are situations where there is no information about P(E), then marginalisation, i.e. the sum of probabilities of all events, can be used [10]. If there is a strong prior belief that some hypothesis is true, then after having

gained more data that fails to support the hypothesis, Bayes' theorem will favour the alternative hypothesis that better explains the data [10].

Attack Graph. An attack graph with a structure of a tree provides a framework to represent information system vulnerabilities and dependencies between them. An attack graph shows the possible attack vectors to compromise a given objective by successfully exploiting vulnerabilities in sequence [18]. All the vulnerabilities that form the attack vector must be successfully exploited. There can be several attack paths through the system to reach the main goal. Logical attack graphs rely on the monotonicity principle, i.e. once an attacker has gained privileges, one will not give them away [18]. Monotonicity introduces directed acyclic graphs (DAG), i.e. there is a directed non-circular movement between the structure of nodes [10]. The occurrence of an event in the attack tree is modelled probabilistically. These models contain one or many parameters, which values are known only with uncertainty [13].

Process. BN is a set of variables represented as nodes and the direct dependences between the edges of these nodes. It is in the form of a DAG and has a set of node probability tables (NPTs) [10]. The process of assessing information security risks considers four steps: (*i*) *identification of vulnerabilities* and (*ii*) *creation of directed arcs between them* to form an attack graph, (*iii*) *calculation of NPTs* (i.e. a table of probabilities that represent the probability distribution of the node given its parents [10]) and (*iv*) *calculation of the result* that is the probability of an incident which happens if one or more vulnerabilities become successfully exploited.

2.3 Method Limitations

The comprehensiveness of ISSRM method and BNBAG method is different. Both application of the ISSRM metrics and usage of the BNBAG method have their limitations. On the one hand, it is difficult to determine the objective values of the ISSRM metrics – one needs to rely on the subjective measures given by the field experts and the history evidences (which might be outdated and not suitable any more for the actual assessment). The subjectivity of the input data makes the analysis and the results of the assessment less reliable. In addition, the ISSRM method does not take into account the potential correlations between the system vulnerabilities.

The BNBAG method covers in majority only the system vulnerability analysis and not the other stages of the risk management. In addition, it might include rather complex data gathering process. The capability of gathering data, which requires time and effort, depends on the maturity level of the organisation.

In this paper we propose a hybrid method and argue that it could help to overcome the above limitations.

3 Combining ISSRM and BNBAG

In Fig. 2, the process of assessing information security risk using the combination of a security risk management method and a probabilistic risk assessment method

is presented. It includes 6 stages and consists of 22 steps. Before starting the risk assessment process (a), a team of domain experts and relevant stakeholders need to be engaged into the risk assessment process.

Context and asset identification. Next step (b) is a creation of business process models. The modelling activity helps (c) to identify the business assets and their supporting system assets.

Security objective identification. Next, one needs to define security needs of the business assets (d). This is done in terms of confidentiality, integrity, or availability.

Threat modelling includes analysis of the security threats. One needs to identify the relevant threat agents ((e) and explain the possible attack methods ((f). In literature there exist a number of studies, taxonomies, and libraries to support his stage, e.g., ENISA Threat Landscape Report [7] or Europol Report [8], MITRE's ATT&CK taxonomy [15], Threat Agent Library by Intel Corporation [3], and ENISA taxonomy [6]. Next step (g) is the measurement of the likelihood of a threat. Hence one needs to gather input from experts.

Vulnerability analysis. There exists a number of vulnerability taxono-mies (e.g., OWASP Top 10 [22], Seven Pernicious Kingdoms [28], Common Vulnerabilities and Exposures [17]) that one could apply for probabilistic assessment. The key question is whether the organisation is capable of gathering the relevant data (h). Vulnerability scanning tools, e.g., Nessus tools [27], OpenVAS [19], can be used to gather information. Then the context related vulnerabilities and their prevalence (i.e., the quantity of the certain vulnerability found in tested network and applications) have to be defined (i). Data about the dependencies between the vulnerabilities have to be found (j); possible methods could include constraint-based algorithms based on inductive causation [24], or score-based algorithms [25]. Once the potential dependencies between vulnerabilities are defined (k) and visualised on attack graphs (l), the data about the likelihood of exploit of each vulnerability has to be gathered (m). The (n) probability of a vulnerability is the probability of prevalence multiplied with the likelihood of exploit. The (o) probabilities of dependent vulnerabilities are the marginal probabilities of the vulnerabilities. It is possible to update the posterior probabilities using the Bayes' theorem if new data is gathered (p).

Threat event and impact analysis. Scenario-based threat modelling can be used. The scenario-based threat modelling (q) should consider a potential threat agent with an attack method to exploit a vulnerability. The potentiality of a threat event is the product of the likelihood of the threat and the probability of the vulnerability (r). Impact is considered in terms (s) of confidentiality, integrity, and availability and defined as a value of impact (t).

Risk evaluation. The risk level value is the product of the potentiality of a threat event and the impact value (u). The scenarios have to be prioritised according to the calculated risk level (v).

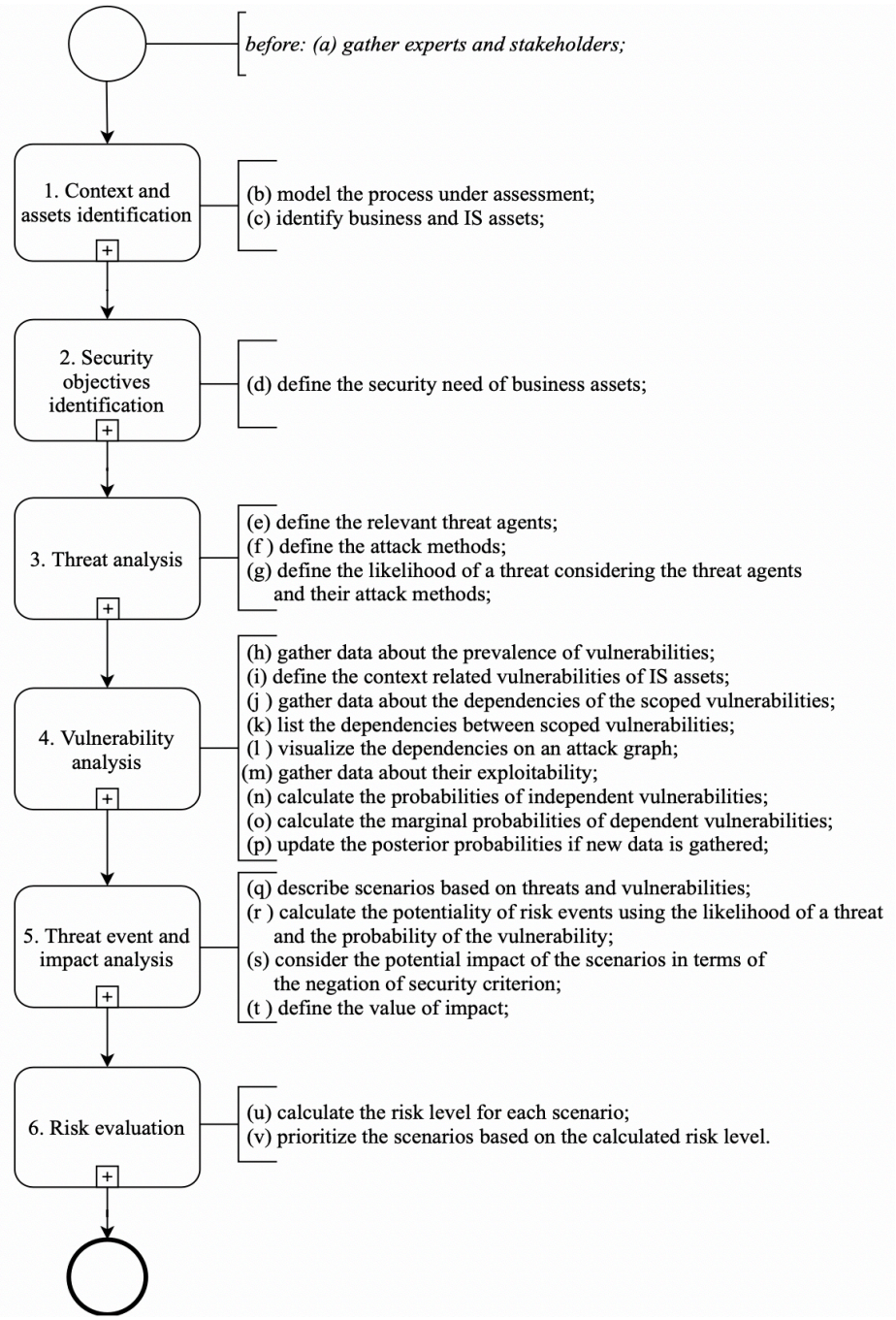

Fig. 2. Security risk management and a probabilistic risk assessment combined

4 Illustrative Example

Context and asset identification. In order to illustrate the proposed alignment, we consider an extract of the outsourcing process in financial institution [23]. More specifically we will analyse the *outsourcing agreement storing* process, shown in Fig. 3.

Threat analysis. According to the ISSRM domain model [5] [14], a threat describes a threat agent who uses an attack method to exploit a vulnerability of the information system asset. In the ENISA report [7], the dominating adversarial threat agents are criminal groups and nation states. And the most commonly used attack methods (see ENISA and Europol [7] [6] [8]): malware, social engineering, distributed denial of service (DDoS), fraud attacks, information thefts and data breaches are notable threats that financial institutions face. In our example we considered these security threats (see Table 1): injection attack, unauthorised access, misuse of information system (IS), phishing, malicious soft-ware, and information gathering.

Table 1. Risk scenarios

Threat	**Vulnerability**	**Impact**
Injection attack: An attacker with a motivation to read Outsourcing agreement from Contract database by sending crafted SQL injection statements though Contract management system.	*CWE89*: Improper neutralization of special elements used in an SQL command in database server.	Negation of confidentiality of Outsourcing agreement.
Unauthorised access: An attacker with a motivation to get Outsourcing agreement from Contract database by running an arbitrary SQL query on database without being authorized to do it and receiving Outsourcing agreement as the result of the query.	*CWE285*: Improper authorization to database.	Negation of confidentiality of Outsourcing agreement.
Misuse of IS: An attacker with a motivation to get Outsourcing agreement from Contract database by having knowledge about the misconfigured database and misusing the legitimately-assigned access rights	*CWE16*: Lack of appropriate access control implementation in database.	Negation of confidentiality of Outsourcing agreement.
Phishing: An attacker with a motivation to exfiltrate sensitive information from Contract management system by embedding a malicious script in URL and sending it as a phishing email to a target user.	*CWE79*: Improper neutralization of input during web page generation in database application.	Negation of confidentiality of Outsourcing agreement. Unreliable *contract management system*.
Malicious software: An attacker with a motivation to read and modify Outsourcing agreement by crafting a malware to exploit known unpatched vulnerabilities.	*CWE937*: Existence of known unpatched vulnerabilities in database server.	Negation of confidentiality and integrity of Outsourcing agreement.
Information gathering: An attacker with a motivation to gather Outsourcing agreement by developing attack vectors to target database information without leaving any trail for forensic analysis	*CWE778*: Insufficient logging of failed login attempts in database server.	Negation of confidentiality of Outsourcing agreement.

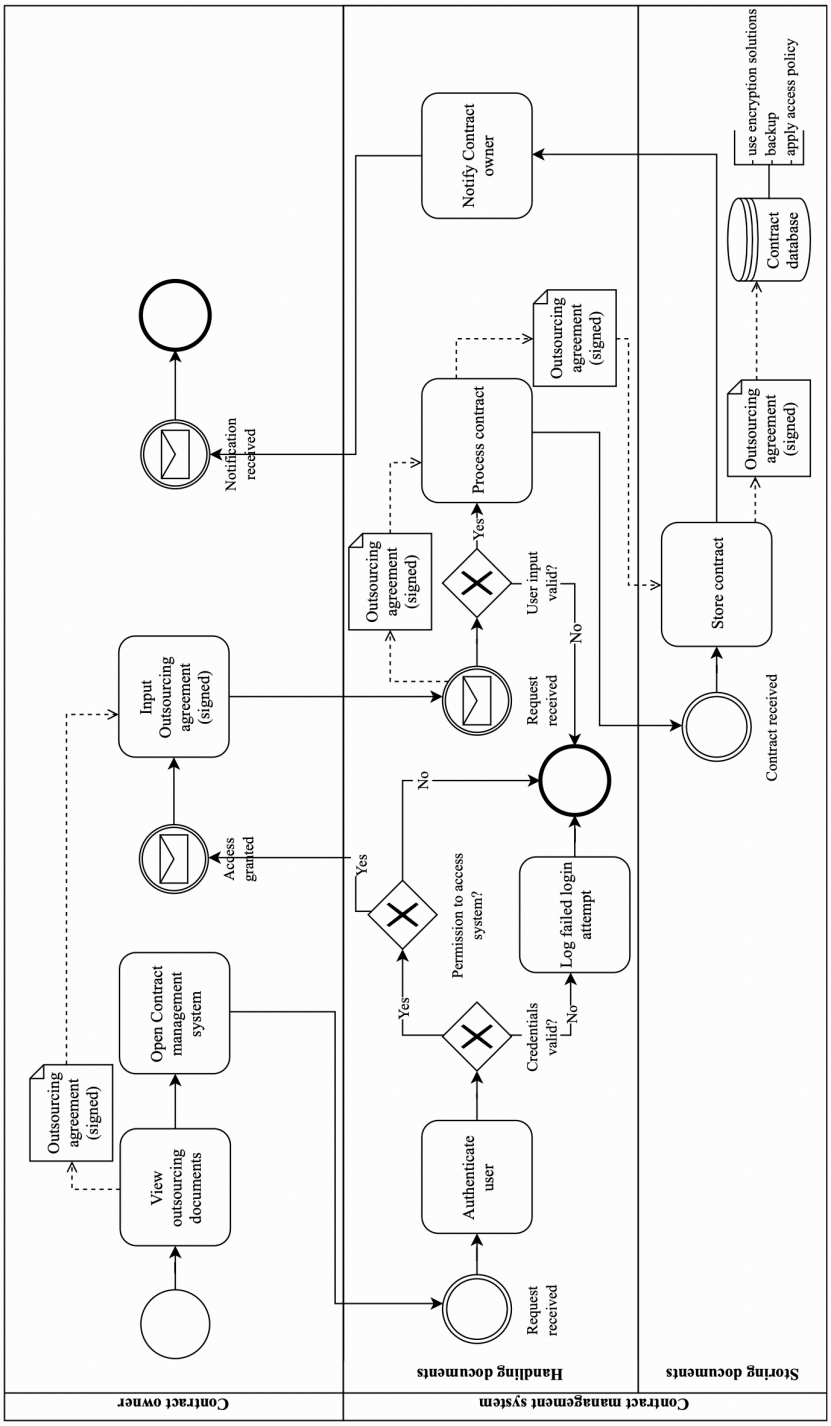

Fig. 3. Outsourcing agreement storing

Vulnerability analysis. In the example we have considered the OWASP top 10 taxonomy [20] to characterise the vulnerabilities of the outsourcing agreement storing. More specifically, this includes (see Table 1): improper neutralization of special elements in an SQL command in contract management system (CWE89), improper authorisation in contract database (CWE285), misconfiguration of access controls in contract database (CWE16), improper neutralisation of input during web page generation in contract management system (CWE79), existence of known unpatched vulnerabilities in contract management system (CWE937), and insufficient logging of failed login attempts (CWE778). Once the vulnerabilities are identified, we have created the vulnerability dependency graph (following the BNBAG guidelines) as illustrated in Fig. 4. For instance, the dependency between CWE285 and CWE16 considers how improper authorisation depends on misconfiguration of access controls.

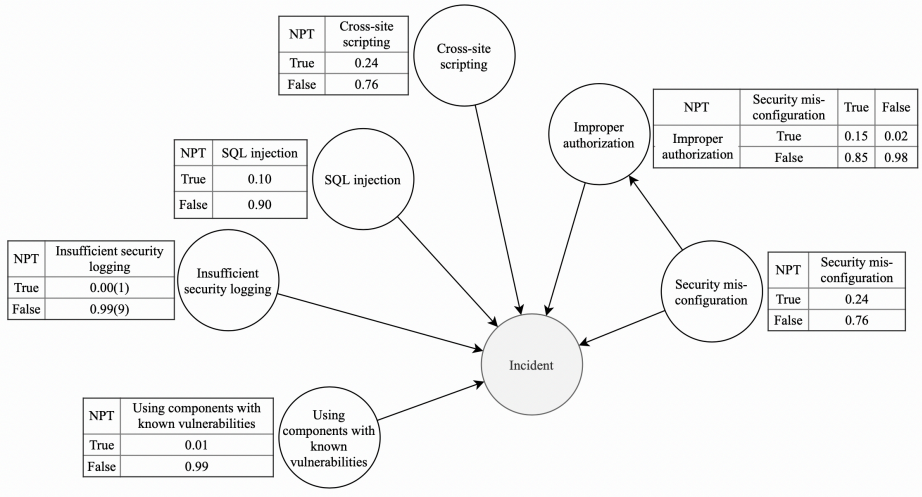

Fig. 4. Attack graph modelling the selected vulnerabilities

The probability of a successful attack by an exploit of independent vulnerability is defined as the product of the *probability of finding the vulnerability in the system* and the *likelihood of its exploit*. Publicly available data provided by the OWASP project [21] is used in the outsourcing scenario for the aver-age estimation of the vulnerability probability. The vulnerability list, which describes the likelihood of exploit using low/medium/high (i.e., 0,2 / 0,6 / 1) is used to estimate the *likelihood of the exploit of a vulnerability* [16].

Next the attack graph illustrates how dependencies between vulnerabilities can be modelled during the risk assessment. An *incident* is defined as the potential compromise of security need. Then the NPTs are formed to calculate the joint probability of the incident, taking into consideration the dependen-

cies between different vulnerability nodes. NPTs provide input for computing the overall probability of a successful incident. NPTs for independent and dependent vulnerabilities are presented in [23] (see Fig. 4). The *true* (T) value represents the probability of an occurrence of an exploit of a certain vulnerability. It is calculated as the probability of the vulnerability being present in the system multi-plied with its likelihood of exploit. The *false* (F) value represents the probability of non-occurrence of such event. The calculations are based on based on OWASP data [21] and MITRE evaluation [16].

Node probabilities of dependent variables are calculated using this equation for prior marginal probability calculation:

$$\mathrm{P}(CWE285{=}T){=}\mathrm{sum}(P(CWE285 \mid CWE16)\mathrm{P}(CWE16))$$
$$\mathrm{P}(CWE285{=}T){=}0{,}15\mathrm{x}0{,}24 + 0{,}02\mathrm{x}0{,}76{=}0{,}05$$

Firstly, CWE285 is dependent on CWE16 as shown by the attack graph. The probability of a successful attack via vulnerability CWE285 is computed for CWE16 being either *true* or *false*. The value *0.05* as the result of the equations indicates that there is a 5% chance that *Improper authorization is true*. The vulnerabilities can be grouped according to their severity (defined as the probability of the vulnerability existing in the system and the likelihood of its ex-ploit). The application of the BNBAG results in the following grouping: (1) Security misconfiguration, (2) Cross-site scripting, (3) SQL injection, (4) Improper authoriza-tion (5) Using components with known vulnerabilities, and (5) Insufficient security logging.

Table 2. Estimation of security risk level

Threat	Value	Risk level calculation					
		Security need	Threat likelihood	Vulnerability level	Potentiality	Impact	Risk level
	max=3	max=3	max=3	max=3	max=5	max=3	max=15
Injection Attack	3	3	3	2.5	4.5	3	13.5
Unauthorized use of software	3	3	2	2	3	3	9
Misuse of IS	3	3	2	3	4	3	12
Phishing	3	3	3	3	5	3	15
Malicious software	3	3	3	2.5	4.5	3	13.5
Information gathering	3	3	2	2	3	3	9

Threat event and impact analysis. According to the ISSRM domain model [5] [14], when a threat agent with an attack method successfully exploits one or more vulnerabilities in a system, it leads to the impact that harms system

and business assets and negates the security criterion. Table 1 represents six security risks to the outsourcing agreement storing stage where a threat agent using the attack method successfully exploits vulnerabili-ties thus leading to the impact. Here the threat categories are assigned using the ENISA taxonomy [16].

Risk evaluation. The results of the security risk assessment are presented in Table 4. Here, the six risk scenarios are evaluated with the metrics provided in ISSRM method. Here security level is refined using the OWASP evaluation [22], threat likelihood is determined after discussion with expert from the financial institution. For simplicity, both value and security need are assessed equally. The evaluation range is from 1 to 5, where 1 is the lowest value and 5 is the highest. In the real-life scenarios the metric values should be estimated based on the history evidences or after the consultation with field experts. In our example we were able to determine some values (e.g., threat likelihood from experts and vulnerability levels from historical evidences), but other ones (e.g., value and security need) were not present.

The results indicate that based on the security risk level, the security risks can be prioritised as follows: (1) *Phishing*, (2) *Injection attack* and *Malicious software*, (3) *Misuse of information system*, and (4) *Unauthorized use of software* and *Information gathering*. This means that the potentially the *Phishing* should be mitigated first, then *Injection attack* and *Malicious software*, and so on.

5 Concluding Remarks

In this paper we analyse how qualitative and quantitative methods could be applied to estimate the security risks. More specifically we analyse the ISSRM and BNBAG methods and illustrate their application in outsourcing agreement storing process. Then we discuss how these methods could be aligned and used together.

The proposed alignment of the ISSRM method and the BNBAG method potentially compensates their individual shortcomings. Firstly, such a hybrid method offers the use of both qualitative and quantitative data as input to the analysis. If the organisation has gained a level of maturity where they have defined the needed data, developed the gathering process, managed it and checked the data quality, then they can use the measurable data as input to the analysis. However, the method does not require the use of quantitative data in all parts of the assessment process. It offers to start with analysing the vulnerabilities based on measurable data and then to use qualitative data in other stages of risk assessment. Additionally, the proposed alignment could be used to consider the potential correlation between system vulnerabilities.

The aligned method is a rather comprehensible in a way that it covers traditional security risk assessment management stages (e.g., risk identification, risk analysis, and risk assessment). The method incorporates the identification of relevant assets, the analysis of the potential threat agents and their attack methods, the analysis of the vulnerabilities and vulnerability dependencies, and the potential impact on the organisation.

The future work includes validation of the proposed alignment. For instance, we will be applying the hybrid method to elicit and assess security risks within other business processes (expressed in different notations).

Acknowledgement. This research has been supported by the Estonian Research Council (grant IUT20-55).

References

1. Õunapuu, L.: Kvalitatiivne ja Kvantitatiivne Uurimisviis Sotsiaalteadustes. Ph.D. thesis, University of Tartu (2014)
2. Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.E.: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon and Software Engineering Institute (2007)
3. Casey, T.: Threat Agent Library Helps Identify Information Security Risks, (white paper), https://pdfs.semanticscholar.org/391e/70510353ba762fa1580a6d9c002eefd2d86b.pdf
4. COSO: Enterprise Risk Management - Integrated Framework, https://www.coso.org/Pages/erm-integratedframework.aspx
5. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. In: Intentional Perspectives on Information Systems Engineering, pp. 289–306. Springer (2010)
6. ENISA: Threat Taxonomy (2016), https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
7. ENISA: Threat Landscape Report 2018 (2019), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
8. Europol: Internet Organised Crime Threat Assessment (IOCTA) 2018 (2018), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
9. FAIR Institute: Measuring and Managing Information Risk: a FAIR Approach, https://www.fairinstitute.org/fair-book
10. Fenton, N., Neil, M.: Risk Assessment and Decision Analysis with Bayesian Networks. Boca Raton: Taylor and Francis Group (2013)
11. Hubbard, D.W.: How to Measure Anything: Finding the Value of "Intangibles" in Business. Hoboken, New Jersey: John Wiley and Sons, Inc. (2007)
12. ISO/IEC: ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management (2018), https://www.iso.org/standard/75281.html
13. Kelly, D., Smith, C.: Bayesian Inference for Probabilistic Risk Assessment: A Practitioner's Guidebook. Springer (2011)
14. Matulevičius, R.: Fundamentals of Secure System Modelling. Springer (2017)
15. MITRE Corporation: MITRE ATTA&CK, https://attack.mitre.org
16. MITRE Corporation: CWE List Version 3.2 (2018), https://cwe.mitre.org/data/index.html
17. MITRE Corporation: CVE Common Vulnerabilities and Exposures (2019), https://cve.mitre.org

18. Munoz-Gonzalez, L., Lupu, E.C.: Bayesian Attack Graphs for Security Risk Assessment. In: IST-153 Workshop on Cyber Resilience (2017)
19. National Institute of Standards and Technology: NIST Special Publication 800-30: Guide for Conducting Risk Assessment. Tech. rep., NIST (2012)
20. Offensive Security: OpenVAS Vulnerability Scanning (2019), https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/
21. OWASP: Official OWASP Top 10 Repository (2017), https://github.com/OWASP/Top10/tree/master/2017/datacall/analysis
22. OWASP: OWASP Top 10. The Ten Most Critical Web Application Security Risks (2017), https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
23. Padur, K.: Information Security Risk Assessment in the Context of Outsourcing in a Financial Institution. Master's thesis, University of Tartu (2019)
24. Pearl, J., Verma, T.S.: A Theory of Inferred Causation (1991), https://ftp.cs.ucla.edu/pub/stat_ser/R156.pdf
25. Scutari, M., Denis, J.B.: Bayesian Networks with Examples in R. CRC Press (2015)
26. Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M.: Taxonomy of Information Security Risk Assessment (ISRA). Computers and Security **57**, 14–30 (2016)
27. Tenable Inc.: The Nessus Family (2019), https://www.tenable.com/products/nessus
28. Tsipenyuk, K., Chess, B., McGraw, G.: Seven Pernicious Kingdoms: a Taxonomy of Software Security Errors. IEEE Security and Privacy **3**(6) (2005)