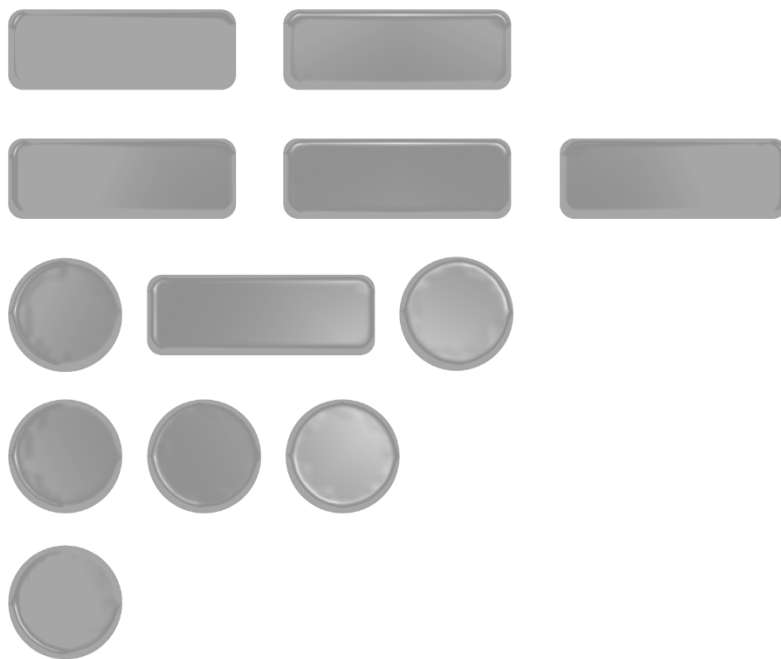


Master Thesis for study program MSc. Business Information
Technology



MORSE

**Model-based
Risk and
Security
Evaluation**

A security risk assessment approach using
Enterprise Architecture models to support
decision-making at Security Operation
Centres

Samir Narain

August 2021

UNIVERSITY
OF TWENTE.



AUTHOR

Samir Narain

Electrical Engineering, Mathematics and Computer
Science (EEMCS)
University of Twente
Faculty : Drienerlolaan 5
7522 NB Enschede
The Netherlands

Study programme : MSc Business Information Technology
Track : IT Management & Enterprise Architecture
Email : s.narain (a) alumnus.utwente.nl
LinkedIn : <https://www.linkedin.com/in/samirnarain>

GRADUATION COMMITTEE

Prof. Dr. M. E. Iacob

Faculty : Behavioral, Management and Social Sciences (BMS)
Department : Industrial Engineering and Business Information Systems
Email : m.e.iacob (a) utwente.nl

Dr. M. Daneva

Faculty : Electrical Engineering, Mathematics and Computer
Science (EEMCS)
Department : Cybersecurity & Safety
Email : m.daneva (a) utwente.nl

Dr. A. Abhishta

Faculty : Behavioural, Management and Social Sciences (BMS)
Department : Industrial Engineering and Business Information Systems
Email : s.abhishta (a) utwente.nl

Henk Jonkers

Company : BiZZdesign B.V.
Department : Research & Development
Position : Research Engineer
E-Mail : h.jonkers (a) bizzdesign.com

Preface

This document is a result of my 8 months master thesis project which marks the completion of my Master in Business Information Technology study. After working for several years in the industry I decided to peruse a master's course to expand my knowledge and also to experience life in a new country. Now that I am at the end of this course, I can very well say that I have achieved both my goals.

My desire to work towards a safer digital society is what led me to take up this project. Having worked on cybersecurity in my early career, this research seemed to blend perfectly where I could apply concepts from my previous work experience and knowledge from academics.

While I am the author of this report, it would not have been possible if I had not been surrounded by some fantastic people. They pushed me to achieve my goals and cheered as I inched closer to finish.

Firstly, I would like to thank BiZZdesign BV for giving me an opportunity to perform this research within their company. I would like to thank Nick Reed, who ensured that the research started on the right track and enabled me with opportunities beyond this project. Even though our conversations were sporadic, they enabled me to maintain focus on the essential aspects. Next, I would like to thank Henk Jonkers, who guided me closely as my supervisor at BiZZdesign. He patiently answered all my questions regarding the research and also beyond to satisfy my curiosity. As one of the developers of ArchiMate, I had already read about his work and was extremely lucky to have him as my supervisor. Our numerous meetings led to important aspects of this thesis and I could get all my doubts cleared whenever I reached out to him. I was also fortunate enough to get close guidance from him on Enterprise Studio scripting, math problems, correct ArchiMate usage among other topics needed for this research. I would also like to thank other colleagues at BiZZdesign who gave their valuable feedback on this research project.

Next, I would like to acknowledge the University of Twente for providing an environment in which students are guided well during their thesis research and studies as a whole. The guidance outside of academics is equally important to complete studies which I could easily find in this university. For my thesis, I was lucky to be supervised by three very accomplished academicians from UT – Prof. Dr. Maria-Eugenia Iacob, Dr. Maya Daneva, and Dr. Abhishta. They guided my research to ensure that it is completed on time and with high academic standards. Their ability to predict what problems I would face in the research process and proactively providing necessary resources needed to continue was essential for my learning. I appreciate the critical feedback and inputs received during the presentations and on my writing. Their familiarity of working with BiZZdesign also gave me a peace of mind that my research was in safe hands. I would also like to mention UT Writing Centre where I frequently dropped by for help with my text.

Next, I would like to thank my friends in the BIT Master's program with whom I could discuss problems and progress. I really liked the close bond we developed even though the classes had moved online in the past two years. Further, I thank Shiva and Suriya for their help with my thesis research.

I would also thank my fiancée Etee for providing emotional support through this time. It was great that she finished her thesis earlier and gave some very important advice on how to finish mine too. Finally, I thank my family for supporting me during my studies.

I hope that you would enjoy reading this document as much as I enjoyed making it.

Samir Narain
Hengelo
31 August, 2021

Executive Summary

As the cyber threat landscape rapidly changes, organizations want to stay updated on how they can protect their valuable assets. Carrying out a risk assessment on their critical asset provides for a way in which organizations can gain visibility on threats and use adequate counter measures to protect these assets. Risk is a function of probability of a negative event happening and the impact that event is going to have when it happens. Traditionally risk assessment has been carried out in a qualitative way where risk is assessed on an ordinal scale. This method is widely used in practice however it has its drawbacks. Ordinal scales: (1) ignore the cognitive bias in people's ability to assess risk, (2) have verbal labels which can be interpreted in a differently by users, (3) are treated as ratios by users which lead to invalid inference, and (4) mostly ignore correlations that would change the relative risks.

For managing cyber threats, organizations establish Security Operations Centres (SOC) that monitor their network for activities that may inflict damages. However, with the growing complexity of Information Systems, malicious actors have plenty of opportunities to attack their targets, and businesses are trying hard to protect themselves. Enterprise Architecture (EA) is used by a growing number of organizations to formalize their structure of complex operations. Through this research we propose a risk assessment approach that supports decision-making in SOC by using Enterprise Architecture modelling. We follow a structured approach called Design Science Research Methodology (DSRM) that has five phases. Initially we carried out problem investigation by performing a Systematic Literature Review of existing academic research on the topics of Enterprise Architecture, Cyber security, and Risk analysis. This resulted in 29 studies that were closely examined and from these we extracted 24 artefacts comprising of 10 risk analysis methods, 7 frameworks, and 7 sets of security metrics. The next phase in DSRM was treatment design where we designed the main artefact of this research.

We introduce the Model-based Risk and Security Evaluation (MORSE) approach which is a six-stage process that leads to a quantitative risk assessment and supports counter measure selection by risk managers at an SOC. In Stage 1, the organization prepares itself for a risk assessment, according to its risk appetite and risk tolerance, and identifies what assets to perform risk analysis on. In Stage 2, they determine the risk, threats and vulnerabilities to the asset and populate metrics. Our approach uses attack-defence graphs which map the probable path an attacker may take to reach their intended target. These are also created in this stage. In Stage 3, the risk analysis is performed in which, using definitions by FAIR (Factor Analysis of Information Risk), the inherent risk, Loss Event Frequency and Loss Magnitude are calculated. In Stage 4, the risk for the asset is evaluated, with respect to the overall risk in the organization, by colourizing elements in the EA model. In Stage 5, risk treatment is carried out which involves selecting and applying control measures to the risk scenario. This is done by selecting controls from a catalogue displayed in a portfolio scorecard view and adding them to the attack defence graph. The selection of controls is supported by a Return on Security Investment calculation that displays the expected effect of the control in the risk scenario based on control strength and control cost. Finally, the total risk exposure is updated in this

stage. The final stage, Stage 6 is a continuous process of monitoring risk. In this stage, relevant decision-makers are periodically informed about the risk in a form through which they can take action to reduce it. Additionally, SOC personnel update the risk scenarios with any change in the risk scenario and the risk assessment can be repeated.

Following DSRM, the next phase was for treatment validation that we carried out in BiZZdesign Enterprise Studio. We demonstrated the approach by performing each task in MORSE and then applying it to an example attack scenario. In this phase, we also examined how the initial requirements were satisfied from the proposed design. The result was all the requirements were either completely fulfilled or partially fulfilled. The final stage of DSRM was implementation evaluation that was performed by conducting a mini-workshop. Five experts were gathered and presented with MORSE. They were then asked to fill out a questionnaire consisting of eight questions that measured their intention to use the approach and perception on how it would work in practice. Their responses indicated that the approach can be applied in real-world scenarios. Certain feedback received during the workshop were also incorporated in this report to improve communicating intended use of MORSE.

Lastly, this research provides recommendations that the approach can be supplied as an example in BiZZdesign Enterprise Studio. This would require certain areas to be researched in-depth, particularly the calculation of risk using probability density functions, Monte Carlo simulation, sensitivity analysis of the inputs, confidence interval in outputs and further improvements in control measure selection.

Table of Contents

Preface	iii
Executive Summary.....	v
Table of Contents.....	vii
List of Tables	x
List of Figures	xii
1. Introduction	1
1.1. Motivation for this research.....	1
1.2. Gap in research.....	2
1.3. Research objective.....	3
1.4. Research questions.....	3
1.5. Structure of this report.....	4
2. Background	5
2.1. Enterprise Architecture	5
2.2. ArchiMate	5
2.3. Enterprise Security and Risk Management	6
- Risk assessment.....	8
- Security Controls	9
2.4. Attack defence graphs	9
2.5. Security Operation Centres (SOC)	10
2.6. SIEM, SOAR and XDR	10
2.7. Enterprise Studio	10
2.8. Lucid chart	11
3. Research Design	12
3.1. Problem investigation.....	13
3.2. Treatment design.....	13
- Requirements	13
3.3. Treatment validation	14
3.4. Treatment implementation	15
3.5. Implementation evaluation	15
4. Literature Review	16
4.1. SLR Research Questions	16

4.2.	SLR Research Method	17
-	Concepts and keywords	18
-	Search for literature	19
-	Screen for inclusion	20
-	Selection of articles	20
-	Quality assessment	22
-	Extract data	22
4.3.	SLR Results	22
-	Concepts	23
-	Methods	23
-	Frameworks	26
-	Metrics	28
4.4.	Additional prior work	31
5.	Design	33
5.1.	Business Scenario	33
	Attack Scenario 1	33
5.2.	The MORSE approach	35
	Stage 1: Prepare for risk assessment	37
-	Define risk appetite and risk tolerance	37
-	Identify assets at risk	38
	Stage 2: Risk identification	40
-	Determine vulnerabilities and threat events	41
-	Populate metrics	43
-	Attack-Defence graph & scenario creation	48
-	Fill / Compute probability of success	52
	Stage 3: Risk analysis	56
-	Compute inherent risk	56
	Stage 4: Risk evaluation	60
-	Evaluate risk with risk appetite and risk tolerance	60
	Stage 5: Risk treatment	62
-	Select and apply controls	63
-	Compute Residual risk	69
-	Calculate the return on security investment	70
-	Compute total risk exposure	71

Stage 6: Monitor risk.....	71
- Inform decision-makers	71
- Monitoring risk.....	72
5.3. Comparison with ERSM process.....	73
5.4. Conclusion	75
6. Demonstration	76
Attack scenario 2.....	76
6.1. Stage 1 – Prepare for risk assessment.....	77
6.2. Stage 2 – Risk identification.....	78
6.3. Stage 3 – Risk analysis	81
6.4. Stage 4 – Risk evaluation	82
6.5. Stage 5 – Risk treatment.....	83
6.6. Stage 6 – Monitor risk.....	87
6.7. Requirements satisfied	88
7. Evaluation	91
7.1. Evaluation structure	91
7.2. Participant profile	91
7.3. Questionnaire	92
- Construct definitions	93
- Scale	94
7.4. Results.....	94
7.5. Discussions during the workshop.....	100
8. Conclusion.....	103
8.1. Limitations	107
8.2. Contribution to scientific research	108
8.3. Implications in practice.....	108
8.4. Future research	109
8.5. Recommendations	110
Appendix 1	112
Appendix 2	115
References	121

List of Tables

<i>Table 1 Structure of this report</i>	4
<i>Table 2 Functional requirements</i>	14
<i>Table 3 Non-functional requirements</i>	14
<i>Table 4 Concepts and keywords</i>	19
<i>Table 5 Data extraction form</i>	22
<i>Table 6 Proposed risk analysis methods</i>	23
<i>Table 7 Framework and models extracted from selected papers</i>	27
<i>Table 8 Metrics identified in the articles included in this systematic literature review</i>	28
<i>Table 9 Stage 1 - Define risk appetite and risk tolerance for the organization</i>	37
<i>Table 10 Stage 1 - Identify assets at risk</i>	39
<i>Table 11 Stage 2 - Determine vulnerabilities and threats</i>	43
<i>Table 12 Stage 2 - Populate metrics</i>	48
<i>Table 13 Stage 2 - Create Attack-Defence graphs</i>	51
<i>Table 14 Estimations of Probability of Success for reference</i>	52
<i>Table 15 Fill / compute probabilities of success</i>	55
<i>Table 16 Stage 3 - Compute inherent risk</i>	60
<i>Table 17 Stage 4 - Evaluate risk with risk appetite and risk tolerance</i>	62
<i>Table 18 Stage 5 - Select and apply controls</i>	68
<i>Table 19 Stage 5 - Compute residual risk</i>	70
<i>Table 20 Stage 5 - Compute Return on Security Investment</i>	70
<i>Table 21 Stage 6 - Compute total risk exposure</i>	71
<i>Table 22 Stage 6 - Inform decision makers</i>	72
<i>Table 23 Stage 6 - Monitoring risk</i>	73
<i>Table 24 Comparison of MORSE with ERSM</i>	74
<i>Table 25 Functional requirements validation</i>	89
<i>Table 26 Non-Functional requirements validation</i>	90
<i>Table 27 Participant's profile</i>	92
<i>Table 28 Evaluation questionnaire</i>	93

<i>Table 29 Summary of evaluation questionnaire responses</i>	95
<i>Table 30 Concepts identified in articles</i>	112
<i>Table 31 Response Q1: The proposed approach is easy to use in practice.</i>	115
<i>Table 32 Response Q2: The proposed approach is compatible with existing customer use cases for risk and security.</i>	116
<i>Table 33 Response Q3: The proposed approach adequately captures business impact for a risk.</i>	116
<i>Table 34 Response Q4: I would be able to find adequate knowledge and support about applying the approach in practice.</i>	117
<i>Table 35 Response Q5: The approach captures the propagation of cyber risk effectively in Enterprise Architecture models.</i>	118
<i>Table 36 Response Q6: The proposed approach would allow for better selection of control measures to mitigate risks.</i>	118
<i>Table 37 Response Q7: Applying the proposed risk quantification approach improves the ability to communicate about risk within an organization.</i>	119
<i>Table 38 Response Q8: Using the proposed approach at a Security operations centre would lead to improved decision-making when responding to threats.</i>	120

List of Figures

Figure 1 The ArchiMate 3.1 full framework [11].....	6
Figure 2 ERSM process for qualitative risk assessment by Jonkers and Quartel (2016) [14]	8
Figure 3 Engineering cycle from Wieringa (2014) [6]	12
Figure 4 Validation model transferred to real world implementation by Wieringa (2014) [6]	15
Figure 5 Systematic Literature Review process from Xioa and Watson (2019) [22]	18
Figure 6 Inclusion and exclusion criteria	20
Figure 7 Article selection process.....	21
Figure 8 Dependency graphs approach proposed by Innerhofer-Oberperfler and Breu (2006) [50].....	32
Figure 9 ArchiMate View for Webshop	34
Figure 10 The MORSE approach overview	35
Figure 11 Detailed process diagram for MORSE approach.....	36
Figure 12 Motivation for risk appetite and risk tolerance	38
Figure 13 Identifying assets in the model	39
Figure 14 Relationships in the MORSE approach derived from Risk and Security overlay	40
Figure 15 Risk and Security overlay metamodel from BiZZdesign support documents [55] ...	41
Figure 16 Risk propagation across layers in Attack scenario 1.....	42
Figure 17 Forms of Losses in Open FAIR, RiskLens via FAIR Institute [56]	45
Figure 18 Entity relationship diagram of ArchiMate concepts and custom defined metrics ..	47
Figure 19 A reference attack graph with various relationships.....	50
Figure 20 Risk scenario created for Attack scenario 1	51
Figure 21 Propagation of Probability of success in simple graph	54
Figure 22 AND decomposition	54
Figure 23 OR decomposition	54
Figure 24 Example of propagation of Probability of Success in an attack graph	55
Figure 25 Open FAIR Risk Taxonomy abstraction from O-RT v3 [13]	56
Figure 26 LEF calculation example.....	57

<i>Figure 27 LEF calculation example with multiple threat events</i>	58
<i>Figure 28 Example risk calculation on attack graph</i>	59
<i>Figure 29 Colour view based on risk appetite</i>	61
<i>Figure 30 SOC Operations Architecture</i>	66
<i>Figure 31 Controls realized from SOC tools</i>	67
<i>Figure 32 Portfolio scorecard of controls</i>	68
<i>Figure 33 Organizational Risk appetite and Risk tolerance set</i>	77
<i>Figure 34 Total view attack scenario 2</i>	78
<i>Figure 35 Vulnerabilities and threat identification for attack scenario 2</i>	79
<i>Figure 36 Attack graph for attack scenario 2</i>	80
<i>Figure 37 Attack graph with probabilities of success filled and computed</i>	81
<i>Figure 38 Attack graph with inherent risk calculations added</i>	82
<i>Figure 39 Risk evaluation through colour view for attack scenario 2</i>	83
<i>Figure 40 Attack defence graph for attack scenario 2</i>	84
<i>Figure 41 Portfolio scorecard of controls</i>	84
<i>Figure 42 Residual risk calculations for attack scenario 2</i>	85
<i>Figure 43 Return on Security calculations on attack scenario 2</i>	86
<i>Figure 44 Updated risk exposure for ArchiMobile</i>	86
<i>Figure 45 Dashboard for communicating with decision makers at ArchiMobile</i>	87
<i>Figure 46 Monitoring risk for attack scenario 2</i>	88

1. Introduction

According to the World Economic Forum's Global Risk Report 2021, cybersecurity failure is the top technological risk society faces today [1]. People live in the digital age where much of the services are provided over the internet, and protecting them becomes vital. Anyone holding assets is under stress to protect them. That is particularly true for large entrusted groups like nation-states and businesses fighting threats from different fronts. It becomes essential for such groups to consider the risks they face and design sufficient countermeasures to mitigate their impact.

As there is a threat to all these from malicious actors, organizations must put specific controls to mitigate such risks. To know an ideal risk mitigation strategy for these threats, it becomes crucial to understand how vulnerable the asset to protect is. Threat modelling is a process that deals with identifying such vulnerabilities in assets, and it can as such be applied to modern-day enterprises that use Information Technology (IT) to accomplish their business objectives. Diagrams that represent such models are called architecture diagrams, and when these are expanded to cover an entire organizations' functioning, they are part of the discipline of Enterprise Architecture (EA). A more accurate definition of terms used in this thesis is provided later in the report.

A recent increase in supply chain attacks in which software from vendors is exploited to enter organizations also poses a serious threat. Companies need to stay updated on the vulnerabilities in their systems, even when they cannot directly rectify them. They can, in turn, put safeguards, control measures, which keep the risk in check. Thus, making it even more critical to have a holistic overview of IT for ensuring sustained operations of businesses.

Through this research report, we communicate how we aim to contribute towards a safer society.

1.1. Motivation for this research

There is an increase in the complexity of attacks on organizations in recent times. Companies need to know what processes are at risk and how they can be protected to minimize uncertainty in business operations. With new vulnerabilities detected every day, it is a proactive job to stay updated. Complex organizations use enterprise architecture for storing their current and future state. Combining that with risk and security concepts allows companies to make proactive decisions based on a complete picture.

A 2019 article by McKinsey & Company highlights the shift organizations are taking to measure cybersecurity from a maturity-based approach to a cyber risk-based approach [2]. They argue that while a maturity-based approach would help companies build capabilities, strengthening essential security and resilience capacity to cover holes, a risk-based approach is an advanced stage for them. A risk-based approach allows organizations to 'identify,

prioritize, deliver, manage and measure security and privacy controls in line with ERM frameworks'. They further present the importance of risk appetite in reducing enterprise risk by prioritizing the selection of controls.

As the rate of cyber-attacks is increasing, there is a greater need to respond to them on time. Manual response to cyber-attacks is no longer sufficient. Thus, there is a need to make quick decisions based on threats and risk profile of organizations. Furthermore, as enterprises are rapidly shifting more of their services delivered through the internet, it increases their attack surface. This motivated our research to support decision-makers in Security Operation Centres (SOC) dealing with a growing number of cyber-attacks while working on limited resources. Risk quantification allows for traceable decision-making, which is near-real-time [3]. By providing ways to security personnel on where to focus their resources, the organization can make more informed decisions and improve their resource utilization.

In this work, we would combine the topics of Enterprise Architecture, risk quantification, cost-benefit analysis, and portfolio management for creating an approach that would support the goal of managing cyber risk for an organization. Because of the nature of EA, which allows complex organizations to be modelled, our approach would use it as a basis for carrying out a risk assessment. Cyber risk, a form of operational risk in organizations, can be quantified following our approach, which leads to better decision-making for selecting an optimal risk mitigation strategy. We focus on optimizing the cost of controls that an organization must maximize its benefits by proposing a portfolio-based approach. Further, using EA models, the propagation of risk in different layers of the enterprise is also realized.

1.2. Gap in research

The topic of risk in connection with Enterprise Architecture has been studied, but these have mainly focused on the qualitative aspects of risk. However, in general, this method of scoring risk has its flaws, which Hubbard and Evans (2010) have highlighted [4]. These are,

1. *"They do not usually take into account the findings of psychological research concerning the cognitive biases that impair most people's ability to assess risk.*
2. *The verbal labels used in ordinal scales are interpreted extremely inconsistently among different users and by the same user.*
3. *Many users treat these scales as if they are ratio scales, with the result that they draw invalid inferences.*
4. *Simple scoring methods rarely consider correlations that would change the relative risks."*

Current EA modelling languages like ArchiMate can support risk management. The Open Group has proposed how these can be defined using existing ArchiMate concepts [5]. This approach is implemented within BiZZdesign Enterprise Studio, which includes risk-related attributes based on the Open FAIR standard. However, this approach is based on an ordinal scale which only lets users perform a qualitative risk assessment. As mentioned earlier, businesses find it challenging to assess the specific risk modern-day cyber threats pose to

assets using existing risk assessment methods. Further, the lack of quantitative methods impedes sound decision-making for security investment as business executives do not understand it.

1.3. Research objective

The main goal of this project is to design a risk assessment approach that would improve decision-making in Security Operation Centres (SOC). A methodological approach is taken in this study based primarily on Design Science Research Methodology (DSRM) by Wieringa (2014) [6]. The research methodology is explained in greater detail later in a separate chapter. We formulate a primary goal to guide our research which is given below:

Primary Goal: *Improve decision-making at Security Operation Centres (SOCs) through enterprise architecture by designing a model-based risk assessment approach.*

Following the DSRM approach, we achieve this goal by answering research questions.

1.4. Research questions

To reach our primary goal, we have defined the main research question as follows,

Main RQ: How to improve decision-making at Security Operation Centres (SOCs) through an EA model-based risk assessment approach?

For answering the main research question, we define seven sub-research questions that combine to reach a conclusive answer. These research questions and their sub-questions are listed below,

- **RQ 1:** What is the current state of research relating security risk with Enterprise Architecture models, according to scientific publications?
- **RQ 2:** What is the current state of research regarding the quantitative and qualitative assessment of the business impact of security incidents, according to scientific publications?
 - **RQ 2a:** Which frameworks are available to describe the types of impact?
 - **RQ 2b:** What are the types of costs associated with security incidents?
- **RQ 3:** How can the business impact be measured for a security incident?
 - **RQ 3a:** Which metrics/KPIs can be defined, aligned with the types of impact?
- **RQ 4:** What factors influence the choice of control measures and incident response courses of action in an organization?
 - **RQ 4a:** How to relate risk appetite to EA models?
 - **RQ 4b:** Can the elements in EA be related to these factors?
- **RQ 5:** How can we calculate a risk score in Enterprise Architecture models?
 - **RQ 5a:** How does the risk score propagate in EA models?
- **RQ 6:** What is an effective decision-making method in SOC that uses model-based security analysis?

- **RQ 6a:** How to select an appropriate control measure based on the risk score of the business concept?
- **RQ 7:** How would this method benefit a SOC in practice?

We defined the sub-research questions in such an order that we answer them sequentially during the research. These research questions fulfil the different phases of Design Science Research Methodology, which the Research Design chapter explains in greater detail.

1.5. Structure of this report

This Master thesis research was carried out broadly in two university courses. First, the research topics course covered problem investigation and systematic literature review (SLR). We describe these in this Introduction and the Literature Review chapters. After sufficient background knowledge was acquired to begin, the design of the artefact started. The work done during this part of the research is described in Design, Demonstration and Evaluation chapters. This work was done as part of the final project course and followed the DSRM approach. This report covers information generated from both the courses. Table 1 shows the organization of chapters in this report.

Table 1 Structure of this report

Chapter	DSRM phase	Methodology	Research Question
Background	-	-	-
Literature Review	Problem investigation	Systematic Literature Review	RQ 1, RQ 2
Design	Treatment design	DSRM	RQ 3, RQ 4, RQ 5, RQ 6
Demonstration	Treatment validation	DSRM	RQ 7
Evaluation	Implementation evaluation	Unified Theory of Acceptance and Use of Technology (UTAUT)	RQ 7
Discussion	-	-	-
Conclusion	-	-	All

2. Background

This chapter introduces definitions used in this report. It provides a theoretical background into the core concepts needed to comprehend the research effectively. We would be going over the definition of topics and then briefly explain how they are relevant in the context of this research.

2.1. Enterprise Architecture

While there have been several definitions proposed for **Enterprise Architecture**, we would like to follow the one stated by MA Rood as, “An EA is a conceptual framework that describes how an enterprise is constructed by defining its primary components and the relationships among these components.” [7]. The enterprise in EA may also refer to any large and complex entity that may be represented in a model. It can be further categorized as a set of people, information or technology which are performing a business function. It is also important here to differentiate two related concepts in EA, of frameworks and modelling language, which are commonly used. EA frameworks, like Zachman Framework and TOGAF, provide a structure for describing the architecture and how the different architectural domains link with each other. Modelling languages, like ArchiMate, are instruments for description and provide a way to communicate the architecture [8].

2.2. ArchiMate

ArchiMate is a modelling language developed to provide an architectural approach that describes and visualizes different business domains and their relationships. Jonkers et al. (2003) presented the first version of the language in which requirements, principles and definitions for coherent enterprise descriptions were laid out [9]. In a subsequent article, Jonkers et al. (2004) [10] defined the main concepts and relationships that are used to visualize the architectural model across different layers. The ArchiMate language has since undergone constant updates and is currently on version 3.1. It is owned and further developed by The Open Group, which is a global consortium that enables the achievement of business objectives through the adoption of technological standards [11]. ArchiMate consists of a core framework that has three layers – Business, Application and Technology, which each have three aspects – Active structure, Behaviour and Passive structure. These have been expanded in the latest version to include Physical, Strategy, and Implementation & Migration layers, and the Motivation aspect. The full framework as of ArchiMate version 3.1 is shown in Figure 1.

The ArchiMate modelling language enables the effective representation of EA through visual diagrams. These diagrams may consist of elements from different layers and joined using relationships that form a meaningful representation of a real-world situation. These relationships are subdivided into four categories – Structural, dependency, dynamic and other. The elements and relationships are presented in views where related concerns of specific stakeholders are addressed. While the ArchiMate specifications themselves do not

have formal semantics for colours, in this research, we use the most commonly used colour scheme – Yellow for the Business Layer, Blue for the Application Layer, Green for the Technology Layer, Purple for Motivation aspects. For the definitions of concepts and relationships used in this research, we would refer [ArchiMate specs](#) document [11].

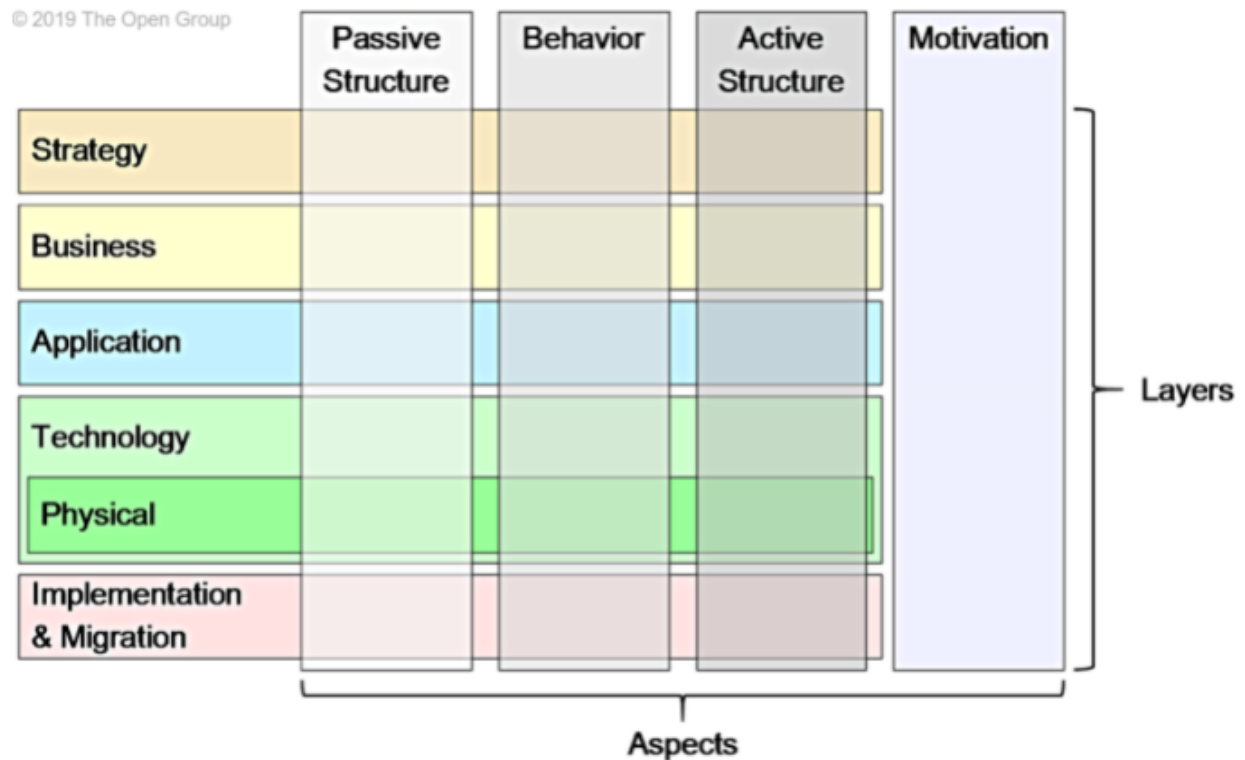


Figure 1 The ArchiMate 3.1 full framework [11]

2.3. Enterprise Security and Risk Management

Large organizations must manage their cyber security and risk posture in the face of growing cyber threats. Enterprise Security and Risk Management (ESRM) includes methods and techniques used by an organization to manage all kinds of risks related to the achievement of their business objectives. Band et al. (2019)[5] published a whitepaper in which they outline how ArchiMate can be utilized to model enterprise risk through the Motivation layer. Model-driven security is a specialization of system architecture design in which models are used for documenting and analyzing security requirements [12]. In this section we define some key terms related to risk and security,

- **Asset** – It is anything that can be owned or controlled to produce value, whether tangible or intangible. An information asset is any data, device or other components in the environment that supports information-related activities.
- **Risk** – There are several different definitions of risk, which makes the process for risk management complicated. However, The Open Group has released a standard taxonomy that intends to establish a common understanding of the terms related to risk. The Risk Taxonomy (O-RT), version 3, defines risk as the probable frequency and the probable magnitude of future loss [13].

- **Vulnerability** – It is the result of analyzing weaknesses of elements in an architecture or component considering the environmental factors that could affect the system [5].
- **Threat event** – When a malicious actor acts adversely against an asset, irrespective of whether they are able to inflict any harm or not.
- **Control measures** – An action, equipment, process, or technique that eliminates or prevents a threat, vulnerability, or attack, or minimizes the harm it can do, or discovers and reports it so that remedial action can be performed.

With EA becoming a mature field of study and more organizations applying its practices, there has been increasing interest in performing risk analysis through it. A study by Jonkers & Quartel (2016) [14] showed how the ArchiMate modelling language could be used to model risk qualitatively in EA models by introducing a security and risk “overlay” to extend functionality. The risk analysis is performed using the Open Fair Body of Knowledge, and the study also shows the application of security aspects in ArchiMate. Figure 2 represents the proposed ERSM process for performing qualitative risk assessment. Our proposed approach is compared with this approach later in this report.

As shown in the figure, the approach by Jonkers & Quartel (2016) has two parts – risk assessment and security deployment [14]. The risk assessment part, represented by red circles on the left-hand side of the image, is based on monitoring, through experience or inspection of the model, potential threats, and vulnerabilities in assets. These can lead to a loss event and pose a risk to the organization. The right-hand side, which is green circles, represent the security deployment phases. It begins with existing security policies that act as inputs for control objectives, i.e., the level of desired protection. This is based on the classification of the information asset, possibly with levels of confidentiality, integrity, and availability (CIA triad). From these control objectives, the organization establishes the requirements for control measures. Finally, these control measures are designed and implemented with the organization. This is the baseline situation, and the cycle can repeat for a new iteration of the ERSM process.

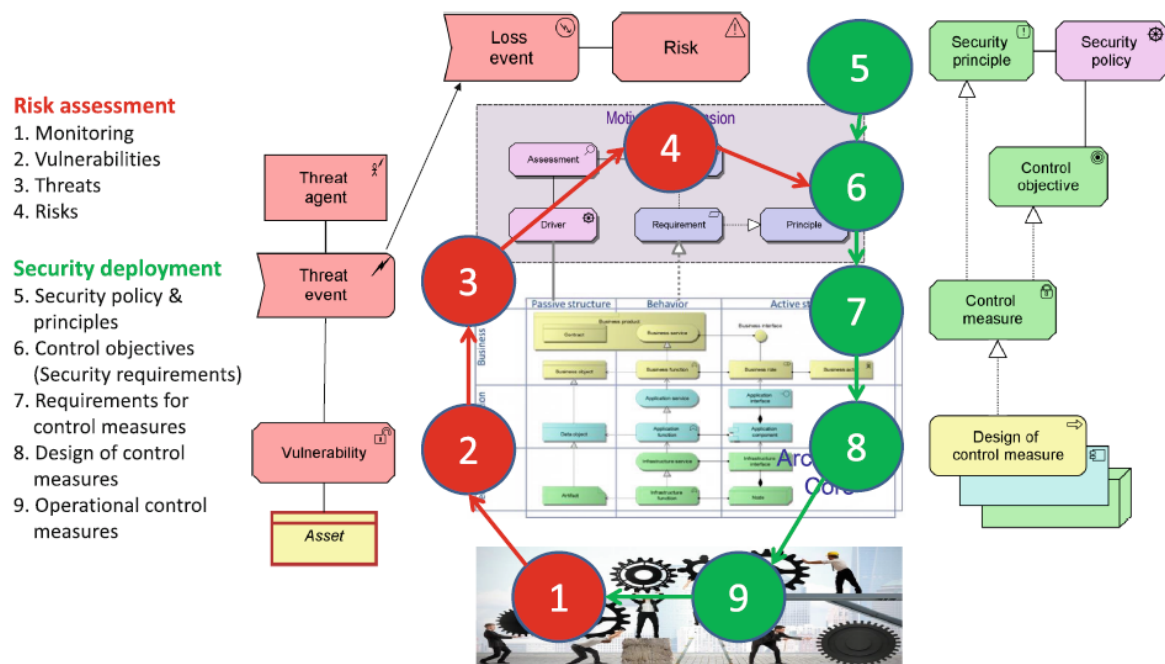


Figure 2 ERSM process for qualitative risk assessment by Jonkers and Quartel (2016) [14]

- Risk assessment

ISO 31000 standard [15] defines risk assessment as the overall process of risk identification, risk analysis and risk evaluation. It is conducted systematically, iteratively, and collaboratively, taking inputs from stakeholders so that the best information available is used which is supplemented by further enquiry if necessary. These three stages are further explained below,

Risk identification – in this part, the purpose is to find, recognize and describe risks that might help or prevent organizations from achieving their goals. In the context of cyber risk assessment, this would include threats and vulnerabilities that affect the digital/IT assets which are necessary for an organization operation.

Risk analysis – The purpose of this phase is to comprehend the nature of risk and its characteristics. A level of risk is defined which considers factors like the likelihood of occurrence, the magnitude of loss, complexity and connectivity, sensitivity and confidence level, among other factors. A qualitative risk analysis is done with ordinal values like high, medium, low versus a quantitative risk assessment that is done with specific estimates of numerical values.

Risk evaluation – The output from risk analysis is used for risk evaluation and in this stage the purpose is to support decision-making on how to respond to the risk. The actions are based on established risk criteria for the organization. The actions could, among others, do nothing further, consider risk treatment, or undertake further analysis.

- Security Controls

The next phase for an organization is to choose how to address the risk by selecting an appropriate treatment option. A treatment would involve changing the likelihood of risk event occurring, changing the loss magnitude, removing the risk source, sharing the risk (with insurance, contracts, etc.), or other manners in which risk would reduce. The selection of treatment options is broader than just based on economic considerations and should take into account the contractual obligations, voluntary commitments and stakeholder views [15].

Security controls are safeguards or countermeasures that are placed to avoid, detect, counteract, or minimize security risk. They are put in order to protect the confidentiality, integrity, and availability of information. There are several frameworks that an organization may adopt depending on their needs. These may be driven by regulatory compliance, or organizations' desire to stay ahead of competition. Some standard controls that organizations may apply are ISO/IEC 27001, CIS Controls, NIST 800-53, COBIT5. These are standards and frameworks which have categories of controls that specify the minimum-security requirements for organizations to be compliant with them.

An example of a control from ISO27001 [16] is - A.12.2 Protection from malware, which is defined in Annex A. The objective of this control is "To ensure that information and information processing facilities are protected against malware". The control is specified as "Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.". Thus, an organization which intends to be certified with ISO27001 must assess and implement this control in their IT environment. The tools with which they reach it is not specified and they are free to choose any software vendor that can provide this functionality.

2.4. Attack defence graphs

Attack defence graphs (or Attack defence trees) are graphical ways for threat modelling i.e., a structured representation of threats and vulnerabilities to a system. They have their origins from fault trees which were used to map a series of events that would lead to a system failure. An attack defence graph consists of an attack tree that is extended with defence nodes. Mauw and Oostdijk (2006) [17] presented an early version of attack trees where they defined them in terms of nodes, its hierarchy, and rules by which manipulation of attack are allowed. Attack trees are further populated with countermeasures to thwart attacks, and these are called attack defence trees (or graphs). We are using the term tree and graph interchangeably in this work as it has been encountered in this way in the literature studied, however they do have a different meaning which is not considered here.

Attack defence graphs also have attributes which are used to measure how successful an attack originated at a leaf node would be in reaching the root node. It includes the probability of success at each node of the graphs, which depends on the vulnerability of the node. If the attacker's capability is greater than the vulnerability of the node, then they have a higher success rate to overcome that and move to the next vulnerability. This continues till the attacker reaches their target which is defined as the root node. Countermeasures placed in the tree try to limit the success of an attacker being able to exploit that particular node.

2.5. Security Operation Centres (SOC)

A Security Operations Centre or SOC (pronounced as /sɒk/ sock or /,ɛs,ʊʔ'si:/ es-oh-SEE) also called Information Security Operations Centre, is a facility where information systems in an enterprise are monitored, assessed, and defended. The SOC is responsible for protecting the IT assets of an organization by using people, processes, and technology. The SOC is generally comprised of security analysts who continuously monitor IT assets of the organization and respond to threats in real time. They do this by scanning logs and events for anomalous behaviour within their network and gather threat intelligence about ongoing exploits. They then respond to incidents to contain cyber threats to ensure that they do not turn into major cyber incidents. In recent days, the pace at which SOC must respond to threats has increased because of rise in automated and targeted attacks to organizations.

2.6. SIEM, SOAR and XDR

SIEM (Security Information and Events Management) is a security solution used by organizations that provides real-time analysis of security alerts generated by network hardware and applications. They work by ingesting logs and events from heterogeneous sources, performing correlation of events and alerting security analyst in case of anomalous behaviour. They also store logs for regulatory compliance and forensic analysis. SOAR (Security Orchestration, Automation and Response) is a technology that is used for incident responses. They provide a way to automate responses by having predefined playbooks or procedures which are executed when a known incident happens. They provide a way to augment human capabilities to allow security analysts to respond faster. SIEM and SOAR tools are commonly found in SOC.

Extended Detection and Response (XDR) solutions provide a SaaS (Software as a service) platform to integrate various security products from different vendors that may be deployed in SOC. A Gartner report published in April 2021 analysis the innovations provided by XDR products and describe their benefits compared to traditional SIEM and SOAR products [18]. While similar in functionality, XDR products provide support for targeted attacks, by including native support for behaviour analysis, threat intelligence behaviour profiling and analytics, which traditional products lack. Both these solutions rely on large amounts of data collected in form of historical logs and real-time events from various applications and devices in the IT landscape. While SIEM is offered as a compliance tool, because of their long-term log storage capabilities, XDR products are provided as an alternative to organizations looking to add threat response to their security capabilities with quick turnaround and limited scope.

2.7. Enterprise Studio

This research project is designed and tested in BiZZdesign Enterprise Studio. It allows for visual modelling for Enterprise Architecture and supports native ArchiMate 3.1 standard. It also extends beyond the basic Open Group standard and provides functionality for customized scripting, portfolio management, and the risk and security overlay that was

utilized in this research. Additionally, it includes Team Server which allows for collaboration on EA models when working in a team. The functionality it provides within Enterprise Studio includes committing, updating, and tracking changes to the model through shared storage places on the cloud. Enterprise Studio (ES) additionally includes modelling in Amber, BPMN, UML among other standards along with a few examples of how it can be used in practice.

Enterprise Studio also offers the use of metrics that are extensively used in this research's design artefact. Metrics are a specialization of the driver concept in ArchiMate which can be used for measurements. These metrics can be linked to both relationships and objects. Additionally, these can be used for scoring elements in a portfolio, and can be filled either manually or automated through scripting logic. We choose to use metrics over defining profile attributes in ArchiMate because of their versatile functionality in ES. BiZZdesign support documents provide a comparison table that helped us solidify using metrics over attributes [19].

Enterprise studio also offers an implementation of the risk and security overlay in ArchiMate. This is supplemented with a qualitative risk assessment which is mentioned in greater details in the ERSM section (of this chapter). This allows for ordinal values for risk-related attributes to be filled in the architecture model and computation of relevant risk values based on Open FAIR standard. However, the implementation is based on O-RT version 1, which is one generation before than the one used in this research.

2.8. Lucid chart

This research includes some diagrams which were created in Lucid charts (<https://lucid.app/>). This is also a diagramming tool like Enterprise Studio, but it's more general-purpose and is offered as a web-based application. For this research, flow charts were created in it using the free version which allows for limited but sufficient functionality.

3. Research Design

In this chapter, we explain how this research was carried out by following a methodological approach. As this research aims to design an artefact that treats a problem, it is a design science project.

This research follows an engineering cycle that is defined by Wieringa (2014) [6] in his Design Science Research Methodology (DSRM) book. Figure 3 shows the steps of the engineering cycle are shown in. The cycle follows almost the same steps as design science methodology by Peffers et. al (2007), and we referred to both articles in our research development [20]. This research follows the method defined by Wieringa because of the questions posed by him for developing a conceptual framework and because of the explicitly defined knowledge questions that should be answered in a typical design science research.

Additionally, Wieringa (2014) [6] provides a template for design problems that is used to define the research objective of this research. The template is provided as,

- *Improve <a problem context>*
- *by <(re)designing an artifact>*
- *that satisfies <some requirements>*
- *in order to <help stakeholders achieve some goals>.*

This template led us to define our research goal, as stated in Section 1.3: *Improve decision-making at Security Operation Centres (SOCs) through enterprise architecture by designing a model-based risk assessment approach.*

The artefact from this research is the risk assessment approach that is proposed in the Research Design chapter. The context that it is applied in organizations which are using Enterprise Architecture models to achieve their objectives.

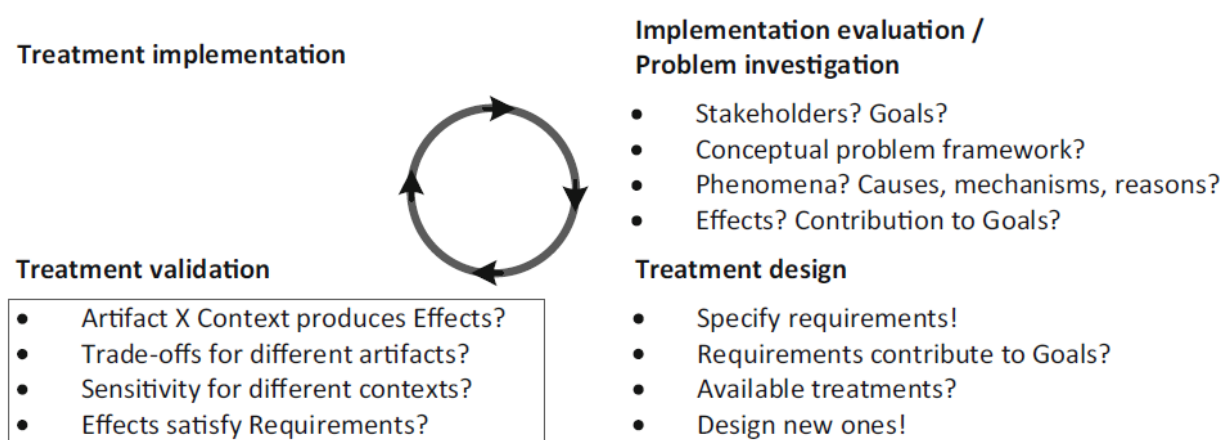


Figure 3 Engineering cycle from Wieringa (2014) [6]

The steps for engineering cycle are expanded on in the following subsections:

3.1. Problem investigation

In the first phase we analyse the problem that this thesis is going to cover. Here we performed an exploratory research. It was identified in the initial phases of research that there is a lack of quantitative risk assessment framework for ArchiMate. As the use of Enterprise Architecture is expanding in large organizations, there comes a need to perform risk assessments also through it. The EA models that companies have include concepts from across the business. These are all vulnerable to growing cyber threat as industries get digitized.

The first phase of this research included looking for existing risk assessment frameworks which are used in the industry and have academic foundation through a literature review process. From these set of frameworks, it was assessed which of them could be applied to EA models on the BiZZdesign Enterprise Studio platform. FAIR methodology showed much promise because of its growing widespread use [21].

3.2. Treatment design

The next phase in the DSRM is to design one or more artefacts that could treat the problem. The design is built based on some requirements that arise from the problem that the stakeholders would like to improve. The requirements contribute to the stakeholder goals. Before designing a new artefact, we also need to look at what are the existing solutions available that can be applied to in the given problem context. If there are no existing artefacts that can satisfy all the requirements, then the next step is to design a new one, which may be a combination of existing options available which satisfy stakeholder requirements.

- Requirements

As part of the treatment design, it is also important to specify requirements for the artifact that should be satisfied. These form the bases on which a treatment is designed as they are specified by the stakeholders of the project who have committed resources (time and money) to it [6]. Requirements in a DSRM are further divided into two types – functional requirements and non-functional requirements. For this research these requirements were gathered in the initial meetings with participants of the project. An initial scope document was created which broadly summarized the outcomes from the project. The requirements were also refined over the period of research when new knowledge was discovered and discussed. The lists of requirements given below were then formed and mapped to stakeholders of the artefact.

Functional requirements

Functional requirements are requirements which define the basic system behaviour. They define what the designed artefact must perform or must not. A function consists of the inputs to the system, its behaviour and the output it produces. They offer a high-level

abstraction for working of the system before it is designed and how the stakeholder goals are going to be fulfilled from each of the requirement.

Table 2 Functional requirements

Sr no.	Functional Requirement
FR1	The approach provides a quantified risk assessment
FR2	The approach is model-based
FR3	The user can perform business impact analysis through it
FR4	The approach supports a way for selecting appropriate control measures
FR5	The approach is based on Enterprise Architecture
FR6	The user can see the propagation of risk through different architecture layers
FR7	The user can do cost benefit analysis of controls
FR8	The approach can be integrated within a Security Operations Centre

Non-functional requirements

Non-functional requirements define the qualities of the artefact. These are supporting the system behaviour in performing its operations in a more efficient manner. These are generally harder to capture as they are not as abstract as functional requirements. These support how the user interacts with the system to ensure it performs adequately for the task it is intended to be used for.

In this research, these requirements were defined so that when the artefact is used by an operator in an efficient manner, without having a steep learning curve.

Table 3 Non-functional requirements

Sr no.	Non-functional Requirement
NFR1	The design can be built reusing existing methods
NFR2	It should be demonstrated in BiZZdesign Enterprise Studio
NFR3	There should be limited number of inputs
NFR4	It can extend the existing ESRM approach in ArchiMate
NFR6	There can be a scenario-based approach to model risk
NFR7	There should be documentation / Training to educate analysts on the proposed approach

3.3. Treatment validation

In the treatment validation phase, we see how the artefact responds in context and if it satisfies the intended design goals. The validation is done on a model of the artefact and is placed in a model of the context to see if the problem is improved by the treatment designed. In this research the validation is done using a sample case study. The proposed artefact is applied on the case study and two attack scenarios are modelled. The model is created in BiZZdesign Enterprise Studio and was presented to domain experts for evaluation in the last phases.

3.4. Treatment implementation

The next step in the design cycle is treatment implementation, which is defined by Wieringa (2014) as “the application of the treatment to the original problem context”. As this research is based on an example case, we do not use implement in an original problem context. However, a model of the treatment is implemented as a validation model, as shown in Figure 4. For an implementation of the research, we would need to apply it to the original problem context in an actual Security Operation Centre and measure the improvements it offers. However, this is out of scope of this research and we move directly to the next step of evaluation of artifact based on the validation model.

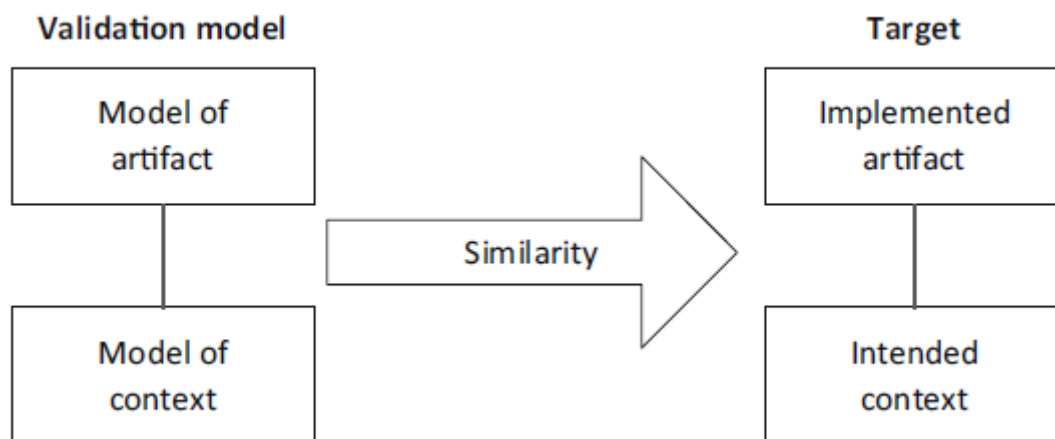


Figure 4 Validation model transferred to real world implementation by Wieringa (2014) [6]

3.5. Implementation evaluation

An evaluation is performed on the designed artefact to test how well it performs in the target implementation. In Implementation evaluation the artefact is tested in the real-world problem context and the benefits are measured. The artefact is evaluated whether it can satisfy the requirements initially laid out. In this research however we are not implementing the artefact in real world scenario. The evaluation for this research is carried out using expert opinion in which domain experts are asked to rate the proposed artefact on certain predefined parameters and provide their opinions. Statistical analysis is performed on the ratings and their opinions are evaluated by the researcher. Some of the feedback provided is also used to improve the design presented within this research.

The next chapter analysis the problem context and state-of-the-art relating to the topics for this research in academic literature.

4. Literature Review

In this chapter, we describe a literature review which is performed for this thesis research. The goal for the review is to collect existing research linking the three main topics for this research. It follows a structured format of systematic literature review (SLR) laid out by Xiao and Watson (2019) [22] to ensure that the topics are covered in breadth through major sources. The methodology laid out by Xiao and Watson (2019) [22] expands on the three step process defined by Kitchenham and Charters (2007) [23], and is shown in Figure 5. Some parts of the SLR were also included from the approach laid out by Webster and Watson (2002) [24], and this would be explained in relevant sub-sections.

This review was performed during the research topics course and submitted as a separate report.

4.1. SLR Research Questions

For conducting the review, we formulated the first two research questions during the initial phase of this research. These contribute to the overall main research question for establishing an academic context. Further a main literature review question is formulated which would be the outcome of this part of research.

Main LRQ: *What is the current state of research relating to Enterprise Architecture, cybersecurity, and risk assessment?*

With this question, we are seeking relevant prior research publications that link together the three main topics – Enterprise Architecture, cybersecurity, and risk. While there is a large number of research publications on these topics individually, there is a noticeable lack of studies linking these three particular topics together, thus the need for performing this research. The main question cannot be, however, answered directly and for this reason, we decomposed it in two sub-questions:

RQ 1: *What is the current state of research relating security risk with Enterprise Architecture models, according to scientific publications?*

RQ 2: *What is the current state of research regarding the quantitative and qualitative assessment of the business impact of security incidents, according to scientific publications?*

RQ 2a *Which frameworks are available to describe the types of impact?*

RQ 2b *What are the types of costs associated with security incidents?*

RQ1 aims to find out the outcomes of research regarding Enterprise Architecture and risk and security.

RQ2 seeks to find the business aspects for decision-making with regards to risks that organizations face. It is further answered by two sub-questions RQ2a and RQ2b. These are chosen as such because RQ2 can be better answered using a more structured approach by

breaking down what constitutes quantitative and qualitative assessments of security incidents. We want to answer this question by getting a deep understanding of the frameworks proposed in scientific literature to describe the business impact of incidents, and of the types of costs incurred due to incidents. In line with these we pose RQ2a and RQ2b.

4.2. SLR Research Method

This section lays out the research methodology used. The literature review is carried out following the process laid out by Xiao and Watson (2019) [22] (see Figure 5), which expands on the three step process by Kitchenham and Charters (2007) [23]. The three major steps are planning the review, conducting the review, and reporting the review. The planning phase involves identifying the need for the review, the problem and research questions, and the review protocol. In the next stage the actual review of articles is carried out. In the final stage, the findings are summarized and reported.

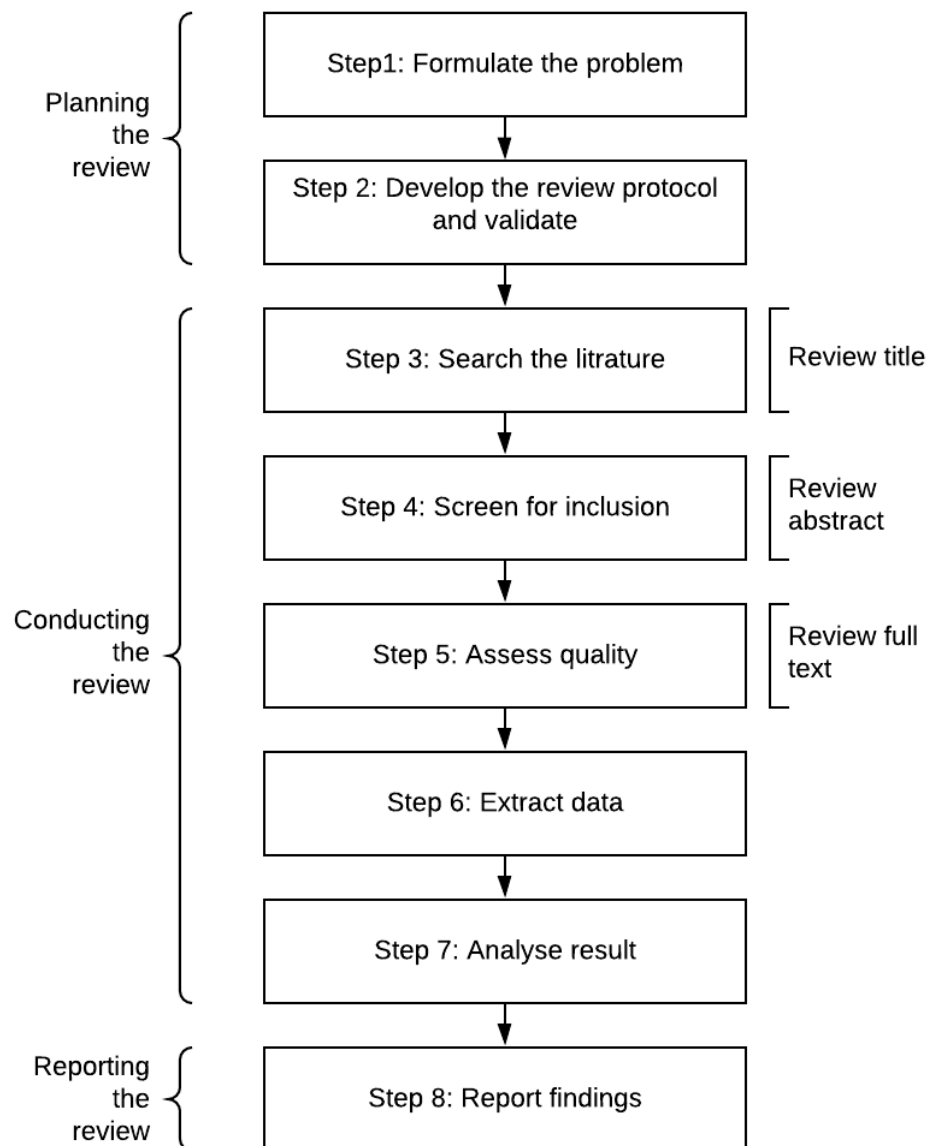


Figure 5 Systematic Literature Review process from Xioa and Watson (2019) [22]

In the next subsections, we describe how our systematic literature review is carried out to answer the research questions listed earlier in this section. The process begins by identifying keywords from the research questions.

- Concepts and keywords

Following the review structure approach defined by Webster and Watson (2002) [24], we aim to identify the main concepts under which the articles would fall, as we would be conducting a concept-centric literature review. These are the broad topics that this research covers, and we identified five such concepts – Business, Enterprise Architecture, Security, Risk

and Analysis. Each of the articles is then marked with which of these concepts are identified in them.

Further, under each of the concepts, we then identified keywords. These keywords formed the bases for creating search queries. The keywords are identified from the research questions by marking the most important words from them. Then exploratory searches are performed using the keywords to some relevant articles. From these articles, synonyms and other keywords are identified, which are then filled in the concept matrix. A combination of these keywords and concepts are used to build the search queries defined in the next section. Table 4 presents these concepts and keywords in a tabulated structure.

The definitions of the EA, Security and Risk concepts are provided earlier in the report, in the Background section. While the other concepts can also be understood from their synonyms, we would like to explain the meaning to avoid confusion on their selection. Articles marked with the 'Business' concept are ones that have a focus on the aspect of cost, improving profitability and generally are in the research area of improving the financial objectives of the organization. Articles that were marked for the 'Analysis' concept would present a framework, model or a method that allows for analytic evaluation of a particular topic.

Table 4 Concepts and keywords

Concepts				
Business	Enterprise Architecture	Security	Risk	Analysis
Business Impact	EA	Cybersecurity	Control measures	Quantitative
Costs	Enterprise Architecture	Cyber-security	Risk assessment	Qualitative
Financial impact	Model-based	Information Security	Risk management	Framework
	Modelling	IT security	Risk score	Assessment
		Security events		Threat modelling
				Business impact analysis

- [Search for literature](#)

We chose two digital libraries of scientific publications for our study: Scopus and Web of Science. These libraries provide the highest impact journals and broad coverage on topics covered in this research. Additionally, we included papers from the Workshop on the Economics of Information Security (WEIS) and the TRES SPASS Project as they include literature relevant to this study. The Open Group Standards on Risk analysis and Risk Taxonomy were also included as they are widely used in the domain but not retrieved through the SLR process.

There were two search queries (SQ1 & SQ2) formed for each of the research questions.

SQ1: ("Enterprise Architecture" OR "EA") AND ("Cybersecurity" OR "IT security" OR "Cyber-security")

SQ2: ("information security" AND "metrics" AND "risk")

The same queries were run on Scopus and Web of Science databases. On Scopus, we searched within "TITLE-ABS-KEY", and in Web of Science, it was performed in the "TS" (topic) field. The search results were exported in CSV format, to be stored and analysed in a spreadsheet, and in RIS format, to be imported in to reference management software. The searches were performed between 28-02-2021 and 03-03-2021.

- Screen for inclusion

Inclusion and exclusion criteria are created for the studies resulting from the search query. Using these criteria, we filter the relevant studies, which directly relate to the research questions. The list of criteria is identified from Kitchenham and Charters (2007) [23] and Aldea et al. (2020) [25].

The inclusion and exclusion criteria used in this review are mentioned in Figure 6. The period for searching the articles was limited to the last 10 years to keep the research based on recent articles and to limit the number of articles retrieved. Important research that was closely related to this study but published more than 10 years back were, however, added to the study as additional articles.

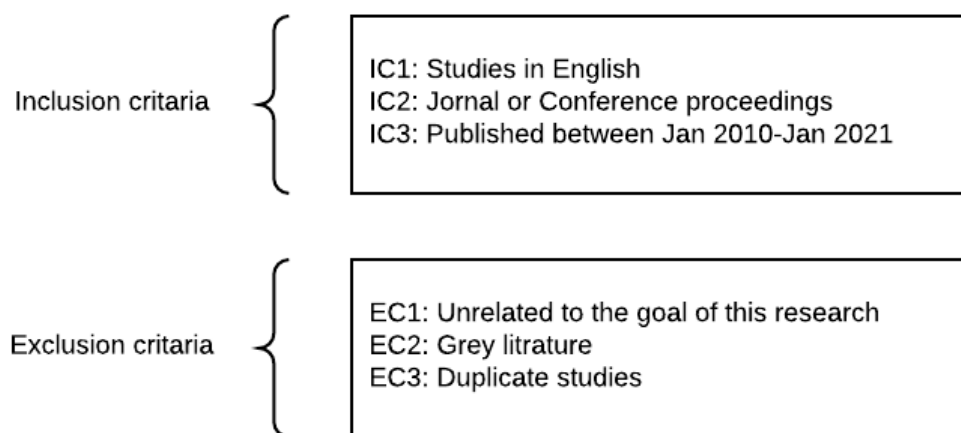


Figure 6 Inclusion and exclusion criteria

- Selection of articles

Following the steps previously defined, the selection of articles for this research is shown in Figure 7 and it is described below.

- a. SQ1 and SQ2 are executed on the two selected digital libraries: Scopus and Web of Science, returning 562 and 72 articles respectively from each of the databases. Of these, 496 were for SQ1 and 138 were for SQ2.
- b. Next, we remove the duplicate entries retrieved from the list of all the articles. There were 55 duplicate records removed, leaving 478 articles for RQ1, and 101 articles for RQ2.

- c. The title of all the remaining records is screened, resulting in 30 articles – 21 for RQ1 and 9 for RQ2.
- d. The abstract of the 30 articles is read to filter which records match the research questions. 20 records remained after this step.
- e. There were 12 additional articles added, which were identified to be relevant for this research. This gave us 32 articles to read.
- f. After reading all the articles, based on the quality assessment, 3 articles were removed. The criteria for assessing the quality of articles for this research is presented in the following section.
- g. The result was 29 articles from which information was extracted and analysed.

Out of these 29 articles,

- 3 are standards
- 9 are journal articles
- 17 are conference or workshop papers

It should also be noted here that not all the articles had methods, metrics, or frameworks, which is why the total number of artefacts extracted is 24. These are presented in section 4.3 SLR Results.

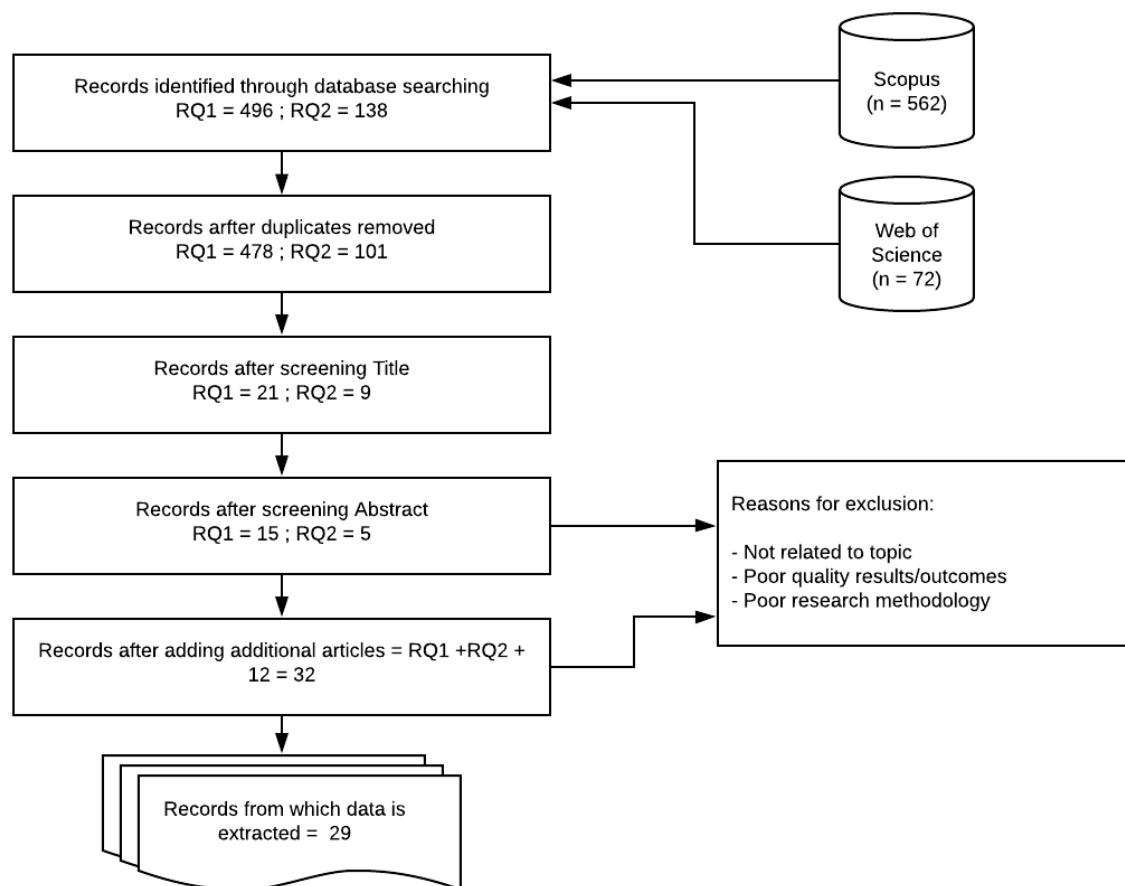


Figure 7 Article selection process

- Quality assessment

The next step in the process was to perform a quality assessment of the studies. The aim for this was to extract data only from studies that are closely related to the scope of this research and limit them to the highest quality studies in the field. It was done by reading the complete text and evaluating them based on the three QA questions we formulated. The questions were based on similar criteria defined by Aldea et al. (2020) [25] and broadly on the guidelines of Xiao and Watson (2019) [22].

- **QA1:** *Does the article relate closely to the goal of this review?*
- **QA2:** *Is there a well-defined research methodology followed in conducting the research?*
- **QA3:** *Does the article include an empirical evaluation of the artefact presented?*

These questions were answered when all the studies were carefully read. It led to the exclusion of 3 studies, which fared poorly in our quality assessment criteria. This, in turn, led to the final selection of 29 articles. These studies which were found to be of suitable quality, were processed for data extraction, as described in the following sub-section.

- Extract data

To extract relevant information from the papers, a data extraction form is created. All the selected articles are read, and the form is filled with relevant information. The form consists of questions that extract general bibliographical information as well as information related to each of the research questions. The data extraction form is presented in Table 5.

Table 5 Data extraction form

Extracted data	Relating to RQ
Title; Author; Publication type; Research methodology; Theoretical or Empirical research	General
Context	General
Method / Framework proposed	RQ2a
Definitions proposed	RQ1, RQ2
Risk / Cost Factors identified	RQ2, RQ2b

4.3. SLR Results

This section presents the findings of the data extracted from the articles following the systematic literature review process. The results are structured as follows: Section 'Concepts' maps the selected articles with the concepts identified in the methodology. Section 'Methods' present the risk analysis methods extracted from the selected articles. We further describe each of the methods in this section. Section 'Frameworks' contains the identified frameworks from the studies. Section 'Metrics' has the metrics that were extracted from the selected articles and we further go on to describe the articles from which the metrics are extracted.

- Concepts

After reading all the selected articles, they are classified based on the concepts which were identified while defining the SLR research methodology. It leads to forming an understanding of RQ1 for the current state of research for security risk and EA. This classification also helped us to look at the articles in a holistic view that facilitated us to easily identify which topics are covered in-depth and which lack sufficient research.

The classification of articles is presented in Table 30 in Appendix 1 because of the size of the table. Here, the number of articles for each of the concept type are summarized below,

- Business: 4
- Enterprise Architecture: 10
- Security: 19
- Risk: 12
- Analysis: 22

Some observation noted from this exercise: no article was retrieved, which includes both enterprise architecture and business together. There is a large proportion of analysis articles, which may be due to the RQ2, in which we are particularly looking for such studies. The number of studies that cover the business concept is limited in the mix of articles.

- Methods

One of the main findings from this literature review is the 10 analysis methods reported in Table 6. These methods distinctly provide ways in which risk analysis is carried out by the various authors, which is summarized in this section. All methods noted below are for performing quantitative analysis.

Table 6 Proposed risk analysis methods

Method	Paper id
Attack Defence Trees	Jhawar et al. (2016) [26]; Sousa et al. (2013) [27]
Attack Fault Trees	Kumar & Stoelinga (2017) [28]
Bayesian Network	Wang et al. (2020) [29]
Breier & Hudec method (unconventional)	Breier & Hudec (2011) [30]
Breu method (Graphs based)	Breu et al. (2008) [31]
Hidden Structure Method (HSM) with Design Structure Matrices (DSM)	Xiong et al. (2019) [32]
Monte Carlo simulation	O-RA v2 [33]
Multi-party computation (MPC)	de Castro et al. (2020) [34]
Petri net-based	Labadi et al. (2020) [35]
Soft goal Interdependence Graphs (SIG)	Zhi et al. (2018)[36]

a. *Attack-Defence Trees*

Three studies utilized Attack Trees in their risk analysis method. Sousa et al. (2013) [27] and Jhawar et al. (2016) [26] use a form of an attack-defence tree and Kumar & Stoelinga (2017) [28] propose a novel approach of using attack-fault trees. These methods provide a graphical way of cybersecurity modelling and are tree-based approaches. An attack-defence tree is one that also includes countermeasures in the form of leaf nodes added to attack-trees Sousa et al. [27]. The Attack-fault tree presented by Kumar & Stoelinga (2017) [28] is useful for cyber-physical systems where the safety aspects of physical equipment can be modelled in the calculations. These methods tend to highlight how the attacker will infiltrate the network and reach the intended target.

b. *Bayesian Networks*

Wang et al. (2020) [29] propose the use of Bayesian Networks on the Open FAIR risk model. This is to eliminate the triangular distribution of input factors and arrive at more accurate calculations for risk calculations, especially for long-tailed distributions. They introduce three models in their study - FAIR-BN, FAIR model risk calculations using Bayesian Network Analysis; FAIR-MC, which uses the Monte Carlo technique as in the original FAIR model, but without the approximations; and EFBN, an extended FAIR-BN technique which incorporates process-oriented and game-theory techniques for making better decisions. The FAIR-BN model allows for using a wider set of input variables compared to the original FAIR model. The results from experimentations performed on the models by Wang et al. (2020) [29] indicate that the FAIR model is the most efficient, FAIR-MC provides more accurate results, and the FAIR-BN model provides higher accuracy while also allowing for modular expandability. The EFBN model demonstrated expandability using process-oriented techniques and defence-attack games, however, it did not show any marked improvement in results over FAIR-BN.

c. *Hidden Structure Method*

The Hidden Structure Method is studied in the context of EA by Xiong et al. (2019) [32] to show how, along with Design Structure Matrices (DSM), it can be used for agile threat modelling. DSM, also referred to as a dependency structure matrix, is a simple representation of a system in the form of a square matrix. For EA, Xiong et al. (2019) [32] use the relationships in the model to be mapped to DSM, as they can be used for directed graphs. By modelling the attacker point of view in the as-is and future state of EA, different DSM are generated. A Hidden System analysis is performed on these DSM to find out the attack vectors and model threats to the system.

d. *Monte Carlo simulation*

The O-RA standard [33, 37] proposes the use of Monte Carlo simulation as one of the methods for risk analysis calculations. Wang et al. (2020) [29] provides a clearer view of the simulations which are employed in the FAIR Risk assessment model. The Monte Carlo method is useful when analyzing data with significant uncertainty. They employ random repeated sampling to generate a probability distribution. The Open Group has implemented FAIR through SIPMath™ distribution in Microsoft Excel and is available as an Open FAIR Risk analysis tool.

e. Multi-Party Computation

In this review, a study by de Castro et al. (2020) [34] was also included, which defines a platform for securely measuring risk in an untrusted environment. While this study doesn't relate directly to our research, it gives insights into how risk-related parameters can be securely shared across a group to form a collective knowledge bank. The proposed secure multi-party computation (MPC) method lets firms input sensitive risk data into the platform without revealing their confidential data to other parties. A statistical computation is performed on data received from all firms, which factors are problematic across the industry. The platform performs risk evaluation on CIS (sub-)controls, and the participating firms can see what are the controls that lead to (max, min, avg, etc.) loss in dollar terms.

f. Petri net-based

A Petri net-based approach for cyber risk modelling and analysis is proposed by Labadi et al. (2020) [35]. Petri net is a modelling language that is used to describe discreet event distributed systems, and is widely used in industrial applications like manufacturing systems, supply chains and logistic systems. In the Petri net-based risk analysis approach defined, there are three steps for risk analysis – modelling, analysis, and mitigation. The approach is applied to an industrial system for demonstrating its applicability and the impact analysis is visualized through the use of graphs.

g. Soft goal Interdependence Graph

Zhi et al. (2018) [36] propose a method based on soft goals to quantitatively evaluate security in architectural diagrams. Soft goals are part of the non-functional requirements (NFR), and in this context, for system architectures. Zhi et al. (2018) [36] proposed an Intra Model Security Assurance approach in which the architecture and security assurances are shown in the same diagram. Extending that approach, weights are applied to the soft goals for the architecture based on organizational and operational criteria. The authors applied this method to a fictional case study about a secure search function on cloud storage, and the NFR of security cases are qualitatively analysed.

h. Other unconventional methods

From the literature review, there were some risk analysis methods identified which did not conform to known methods but were found relevant to be analysed.

Breu et al. (2008) [31] introduce security metrics and explain how they aggregate from the underlying model using graphs. They propose to start elicitation with the identification of a Business Security Objective (BSO), which would be relevant to some elements in the architecture domain. These elements become the root element for the Dependency Graph. These are used to create a Threat Graph for the model. Along with the number of attacks on the system, a proposed algorithm is used to calculate the violation of security requirements. With this number of violations, the ALE (Annual Loss Expectancy) can be calculated using the formula $ALE = ARO * SLE$.

Breier & Hudec (2011) [30] propose to automatize risk analysis based on security metrics, which they say would reduce subjectivity factors for security evaluation and bring objectivity to the risk assessment process. The method they propose is to identify one or more security metrics for each security control. These metrics are provided with a weight. Characteristics for the security metrics are defined, with best case, optimal and worst-case values. Using a formula, the security metric for the control objective is calculated.

i. Impact assessment method

In the study done by Granadillo et al. (2016) [38], they proposed an impact assessment method which we are separately classifying here. They propose a dynamic risk modelling system that takes the response to attacks on ICT systems into risk assessment. The Response Financial Impact Analyzer (RFIA) quantifies the benefits of a response plan on a financial basis, and it is composed of a Return on Response Investment (RORI) component and an Attack Volume engine. The Response Operational Impact Analyzer (ROIA) performs an operational assessment of the response. It is composed of a network dependence analyser, local impact definition and Monte Carlo evaluator. The ROIA supports RFIA by evaluating the response plan and performing an operational analysis on it. The two components, RFIA and ROIA, when combined, support the Dynamic Risk Management Response System (DRMRS), which assesses the success of an attack, financial impact and the impact of the response. The system was applied to an Energy distribution Organization as a case study in [38].

- Frameworks

Sub-question RQ2a was defined as “*Which frameworks are available to describe the types of impact?*”. To answer this question, we extracted the frameworks that the authors of the selected articles intended to describe in their research. This resulted in 7 separate frameworks which are tabulated in Table 7. These were then classified based on the topic they covered – Risk, Risk and Security, Security and Security Cost. We use the topic that a framework covers as a classification label to mark the type of frameworks dealing with the same topic. For example, the frameworks in the first two rows of Table 5 (ASRAaaS and FEA SSPP) cover the topic of Risk, therefore we classify them in the Risk type of frameworks. All frameworks, except the ones with type Security cost, are related to enterprise architecture also. In the next subsections, we will present the frameworks according to the topics that they cover.

Table 7 Framework and models extracted from selected papers

Framework	Topic	Paper id
ArchiMate based Security Risk Assessment as a service model (ASRAaaS) framework	Risk	Abbass (2019) [39]
FEA SPP – NIST Tiered RM Framework	Risk	Nather (2018) [40]
An integrated framework for RM, ISM and EAM	Risk and Security	Diefenbach et al. (2019) [41]
EAM-ISSRM integrated model	Risk and Security	Mayer et al. (2019) [42]
Security Architecture Framework for Enterprises (SAFE)	Security	McClintock et al. (2020) [43]
Security Productivity - Investment Model	Security Cost	Böhme (2010) [44]
Cost of Cybercrime Framework	Security Cost	Anderson et al. (2019) [45]

a. Risk

There are two frameworks which are of type risk, the ArchiMate based Security Risk Assessment as a service model (ASRAaaS) framework [39] and FEA SPP – NIST Tiered RM Framework [40]. Abbass (2019) [39] propose an integration of two frameworks, a preventive risk analysis framework and a responsive risk analysis framework. The preventive risk analysis framework detects network-based attacks, and the responsive risk analysis framework responds to attacks and addresses the risk. Together, along with a mobile agent component, they provide an ArchiMate based approach to perform the risk assessment. Nather (2018) [40] provides a cross-analysis of the FEA-SPP and the NIST Tiered RM Framework. It promotes the need for having enterprise architecture in organizations to align the strategy with and the information security needs and proposes them to be ‘baked in’ to the current and future state architectures. The author gives the example of Netflix and ShareFile, two organizations that used EA for Risk Management and were able to avert disruption to their services by identifying critical dependence on their cloud service provider Amazon Web Services for EC2 instances.

b. Risk and Security

Diefenbach et al. (2019) [41] proposed an integrated framework for RM, ISM and EAM. The framework is based on the ISO standards and introduces additional concepts of risk and asset to link the EA framework with the RM/ISM framework. In their proposed framework, the ISRM ISO standard is also fitted inside the RM&ISM standards. Mayer et al. (2019) [42] present an integrated model for EAM and ISSRM (Information System Security Risk Management). It represents concepts related to asset, risk, and risk treatment from the ISSRM model and concepts from EAM. They also present an alignment table for ArchiMate 2.1 concepts in their study, which maps EAM concepts to the ISSRM domain model.

c. Security

The Security Architecture Framework for Enterprises is proposed in the study by McClintock et al. (2020) [43]. It was developed after the evaluation of 25 existing security

frameworks. It is based on the Zachman Framework and provides security instantiations for all 36 cells. Four factors for each cell are identified – detailed explanation, pictorial model, framework example and compliance mapping (to NIST or ISO27000).

d. Security Cost

Böhme (2010) [44] model is explained in the metrics section. Anderson et al. (2019) [45] have provided an update to their previously presented framework. The framework for analyzing the cost of cybercrime to society is provided in their article, which identifies the different costs categories associated with the crime and how it is divided between the stakeholders - criminals, victims, and society. The framework indicates that:

- Criminal revenue is much lower than the losses the cyber-attack causes.
- Direct loss is the value in loss, damage, or other sufferings to the victim of the cybercrime
- Indirect losses - loss of value and opportunity costs impost on the society because of the cybercrime
- Defence costs - the cost of preventive measures - eg. antivirus, firewalls etc.
- Cost to society on the whole is the sum of Direct losses, indirect losses, and defence costs.

- Metrics

The metrics identified during the data extraction process are tabulated in this section. We found 7 articles that had metrics defined in them. These are presented in Table 8. There were two main types of metrics that we encountered – relating to costs and relating to risk & security.

We would not be defining each of the metrics because their definitions are better provided in the referenced articles. However, we would explain the context in which these metrics were defined and if they were empirically tested with the article or not.

Table 8 Metrics identified in the articles included in this systematic literature review

Extracted metrics	Paper id
Loss Event Frequency - Threat Event Frequency - Vulnerability - Contact Frequency - Probability of Action - Threat Capability - Resistance Strength Loss Magnitude - Primary Loss Magnitude - Secondary Loss - Secondary Loss Event Frequency - Secondary Loss Magnitude	O-RT v3 [13]
- Cost of security - Security level - the quality of protection	Böhme (2010) [44]

<ul style="list-style-type: none"> - Benefits of security <p><i>Costs,</i></p> <ul style="list-style-type: none"> - Onetime cost - Recurring costs - Sunk costs - Fixed - Variable <p>Return on Security Investments (ROSI)</p>	
<ul style="list-style-type: none"> - Probability of disruption - Expected Cost of A malicious disruption - Mean time to malicious disruption - Constrained values - Role of adversaries - design alternatives 	Kumar & Stoelinga (2017) [28]
<p><i>Security Concern</i> for Business Process</p> <p>= $\alpha \times$ Availability Concern for Business Process</p> <p>+ $\beta \times$ Confidentiality Concern for Business Process</p> <p>+ $\gamma \times$ Integrity Concern for Business Process</p> <p>$\alpha + \beta + \gamma = 1$</p> <p>$\alpha$, β, and γ are the weights applied to the respective concerns</p>	Mukherjee & Mazumdar (2019) [46]
<ul style="list-style-type: none"> - <i>Damage %</i> - percentage of nodes impacted - <i>Dispersion</i> - d/D' ; d = maximal diameter of the infected node; D'= Maximal total diameter - <i>Concentration</i> - m/M ; m= number of impacted nodes with at least 2 impacted neighbors M= total number of impacted nodes - <i>Directs</i> - Dir/D ; Dir=directly impacted links ; D=number of links emitting from a node - <i>Seconds</i> - Sec/D ; number of links to working nodes - <i>Disconnection risk</i> - $1/W$; W=number of arcs connected to working nodes 	Weintraub & Cohen (2018) [47]
<ul style="list-style-type: none"> - the percentage of the IT budget spent in information security - the ratio of employees to security staff - the time a critical system is unavailable - the capability of the security team to deal with mature threats - the number of vulnerabilities detected as well as the time spent to reduce them - the average time to resolve security incidents - the number of resources impacted by each security incident 	Pereira & Santos (2014) [48]
<p><i>Mean Failure Cost (MFC) = Matrix multiplication of ST*DP*IM*PT</i></p> <p><i>Calculate stakes matrix (ST)</i> - how much each stakeholder may loose in case of system failure</p> <p><i>MFC(i)</i> - a random variable that is the loss per unit operation time (\$/hr)</p> <p><i>Dependency Matrix</i> - Probability of failing requirement Ri., once component Ck has failed</p>	Aissa, A. et al(2011) [49]

<p><i>Impact Matrix</i> - assessment of the threats affecting the components and the likelihood of success</p> <p><i>Threat configuration</i> - Probability that threat Tq materializes during a unitary period of operation</p>	
<p>Security metrics - an abstract subjective attribute derived from measurement. Good metrics are</p> <ul style="list-style-type: none"> - consistently measured without any subjective criteria - Cheap to gather, possibly through automation - Expressed as cardinal number or percentage - Expressed with atleast one unit of measurement - Contextually specific and relevant to decision-makers 	<p>Breier & Hudec (2011) [30]</p>

The Open Group standard, O-RT v3 [13], provides a taxonomy for information security risk and a logical and rational framework for factors affecting risk. The document was created for security and risk personnel to communicate over a shared language in their profession. The document refers to the ISO Guide 73:2009 for certain definitions, which would give it a wider fit in the IT landscape. The metrics defined in the taxonomy do not require all the values to be provided and only allows for different levels of abstraction based on how it is being applied.

Böhme (2010) [44] propose to decompose the security production function, which is the productivity of security investments, into two parts. They map the cost of security to the security level, and the security level stochastically determines the benefit of security. Further, for the cost of security, they enumerate the various types of costs that can be associated with an investment – onetime cost, reoccurring costs, sunk costs, etc. The author, however, doesn't apply the proposed framework to empirical testing.

As described in section a, Kumar & Stoelinga (2017) proposed the Attack Fault tree method for security and safety risk analysis [28]. They further go on to perform three types of analysis on it –

- as-is, (metrics – Probability of disruption, expected cost of malicious disruption, Mean time to malicious disruption)
- what-if (Metrics – constrained value, the role of adversaries),
- design alternatives (No separate metrics)

Their approach is demonstrated through 3 case studies, so we can say that they validated their research empirically.

Security concern is introduced as a new metric by Mukherjee & Mazumdar (2019) [46]. The basic factor for this metric is the damage potential of exploits against the business process for enterprises in the context of a threat scenario. The security concern metric is made up by confidentiality, integrity, and availability concerns, which would vary depending upon the industry/type of business process. α , β , γ in the equation correspond to weights of the concerns. The authors provide an example on which they apply the security concern metric, which, however, we would consider this study to be theoretical because of the lack of application-based testing for it.

The work by Weintraub & Cohen (2018) aims to make it easier for IT managers to measure the availability of the systems and thus define the aforementioned metrics [47]. The metrics quantify the impact of a cyber-attack on network components and are best illustrated through network diagrams of connected computer nodes. The metrics also allow the managers to assess the impact in case an attack happens and plan preventive activities. The authors do not empirically test the metrics in the study.

Pereira & Santos (2014) proposes security metrics to evaluate the organizational IT security posture [48]. They attempt to bridge the gap through their metrics to bridge the gap between IT and business.

Aissa et al. (2011) propose a single metric, the Mean Failure Cost (MFC) [49]. They attempt to show what failure of a single component would mean in a multi-stakeholder context. They consider the variance of stakes that each stakeholder has in meeting security requirement. The metric is implemented in an automated tool for calculating MFC, however, they do not provide any results of the validation in the article. We would consider that it is a theoretical model because of the lack of testing data.

The use of security metrics for automatizing risk analysis is proposed by Breier & Hudec (2011) [30]. Their method and how the metrics they used are explained in section h of Methods.

4.4. Additional prior work

There were articles that came about during the research, which we would like to mention here. These did not turn up in the searches for the literature review for various reasons but also provide a base for this research. The initial literature review was kept unchanged to limit the time spent on completing the research process.

Innerhofer-Oberperfler and Breu (2006) [50] propose a dependency relationship between different layers of an enterprise by using a dependency graph. It states that there is a dependency relationship for realizing elements in the top most layer, and it is linked to the lower layers. Here, as shown in Figure 8, the layers in order are business, application, technology, and physical layers. This is similar to how the ArchiMate modelling language is, however the authors use UML notation instead. We incorporate the same logic in our design presented in the next chapter that there is a dependency among elements in different layers. However, unlike the approach by Innerhofer-Oberperfler and Breu (2006) [50], we do not use security requirements and instead base it on the security principle element of ArchiMate Risk and Security Overlay (RSO). This saves the risk analyst time from breaking down security requirements for lower layers.

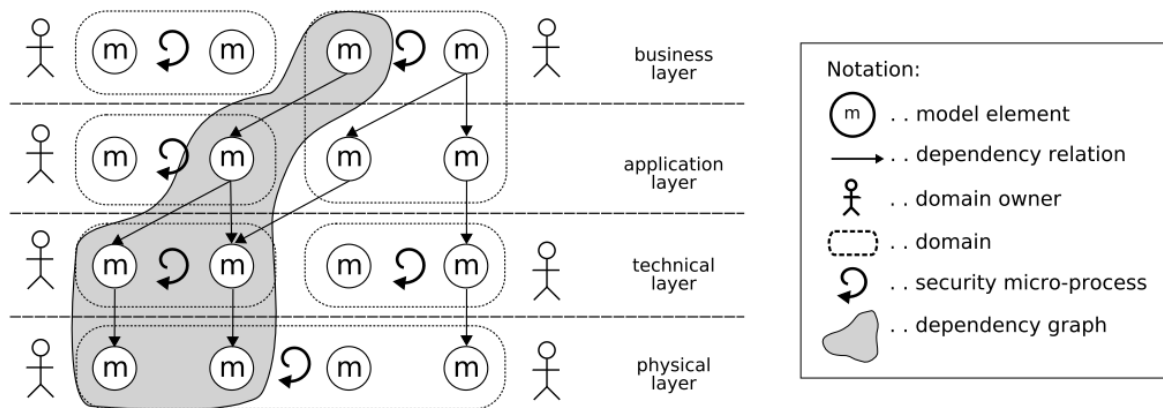


Figure 8 Dependency graphs approach proposed by Innerhofer-Oberperfler and Breu (2006) [50]

Le et al. (2019) [51] introduce a way for hybrid implementation of FAIR with Bayesian networks. They use look up tables (LUT) to derive ordinal LEF, TEF and vulnerability values using cause-and-effect relationships. These are included with fuzzy vectors to generate probabilistic results in the lookup tables. Using a grading vector, these ordinal values are then used to arrive at a numerical value of LEF which can be used for quantitative risk assessment.

Hacks et al. (2019) [52] combine the three domains of model-driven security engineering, attack defence graphs and security modelling in ArchiMate. They expand on their previous work Johnson et al. (2018) [53] in which they proposed a Domain Specific Language (DSL) called MAL (Meta Attack Language) for probabilistic threat modelling and attack simulation. In this work, they are first performing threat modelling in ArchiMate and then they transform ArchiMate models to MAL by using the XML-based exchange format. The junctions in ArchiMate are also used to reflect relationships between attacks and are subsequent translated MAL keeping the same meaning. The MAL includes assets that contain attack steps, representing attacks/threats. These attack steps are linked to form an attack path which in turn are used for creating attack graphs. These attack graphs are then used to run attack simulations.

5. Design

In this chapter of the thesis report, we present our proposed design for the risk assessment approach. The chapter begins with a scenario which is an example case study from which the approach was modelled to support the designing phase of this research. The case study is derived from one view of the Risk and Security example of ArchiSurance (available in Enterprise Studio) and developed further by adding more details. This case study is referenced later in this chapter to show how the various stages of the proposed design can be applied.

5.1. Business Scenario

ArchiMobile is a global mobile manufacturer with a complex corporate structure. They are a subsidiary of a larger enterprise Archi. ArchiMobile produces and sells mobile phones directly to consumers.

As they are a large and old enterprise, they have complex business processes to ensure high standards of quality and efficiency. They are a profit-driven organization with a varied shareholding pattern. To stay ahead of the competition, they are constantly innovating their products and processes. Malicious actors are after the latest technology they develop, and ArchiMobile is fighting hard to keep confidential IP private.

They have an established internal SOC and mature IT practices. As they operate in multiple regions of the world, they need to stay compliant with local regulations. They are a NIST 800-53 compliant organization and have these controls defined in their architecture model. They want to be proactive with their security and prudent with their investments.

It is the responsibility of SOC teams to maintain the overall security of all IT applications within ArchiMobile. But because of the legacy structure, they also have applications that are not protected adequately with security best practices.

The management wants to have more extensive coverage of the applications and what existing security investments can provide them by improving coverage. They have decided to undertake a risk assessment to analyse emerging cyber threats that could potentially impact their business.

Attack Scenario 1

An employee has the task of updating the public-facing website with new product information. The website is for ArchiMobile, and there is a new mobile phone in the market that they will showcase to the public. A database stores the information about the phone, and a Content Management System is in place to manage the public-facing website.

Their competitors and the media seek to gain confidential information about the phone, and the company has controls in place to prevent that.

The business process that the employee uses to update the information is modelled as 'Adapt public website information', which uses a CMS system to process changes to the website. There is an alternate *business process* that 'Anybody' can use to access the website content, 'Browse public website'. This business process is not covered in this risk assessment.

This scenario is modelled as a total view in ArchiMate and is shown in Figure 9. It covers business, technology, and application layers for the webshop of ArchiMobile.

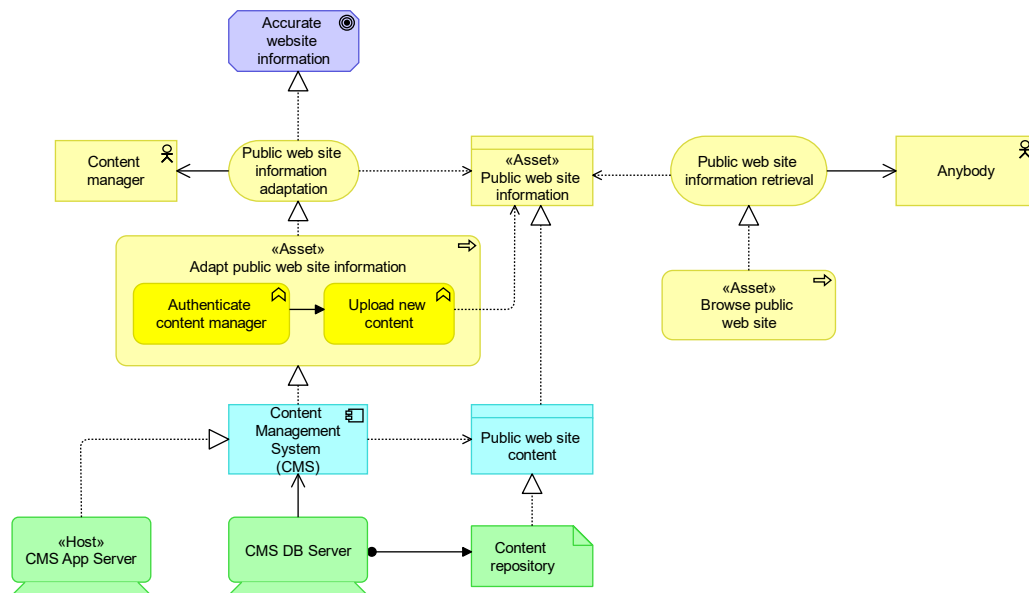


Figure 9 ArchiMate View for Webshop

5.2. The MORSE approach

In this section, we would introduce the **Model-based Risk and Security Evaluation** approach and would refer to it as the MORSE approach. Figure 10 shows the detailed process flow of MORSE. It is a 6-stage process that expands the general risk assessment process that consists of the three basic steps for risk identification, analysis and evaluation as defined in ISO31000 [15] and also used in Open FAIR Risk Analysis [33]. Each of the six stages has further tasks that are to be performed within them. These 6-stages are shown in Figure 10 and explained in more detail in Figure 11. A risk analyst should ideally go from one stage to another, as these are different parts of the risk assessment process, following the directed lines. In the next subsections, we would go over each stage in detail and explain how a risk manager/analyst would accomplish the tasks. While describing each of the tasks, we are following an approach in which the inputs, mechanism and outputs are defined. These are presented in a tabular form at the end of the task description.

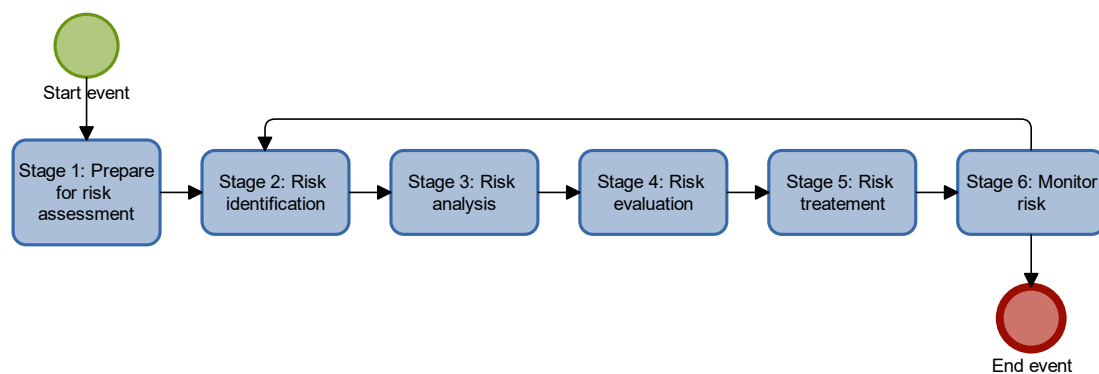


Figure 10 The MORSE approach overview

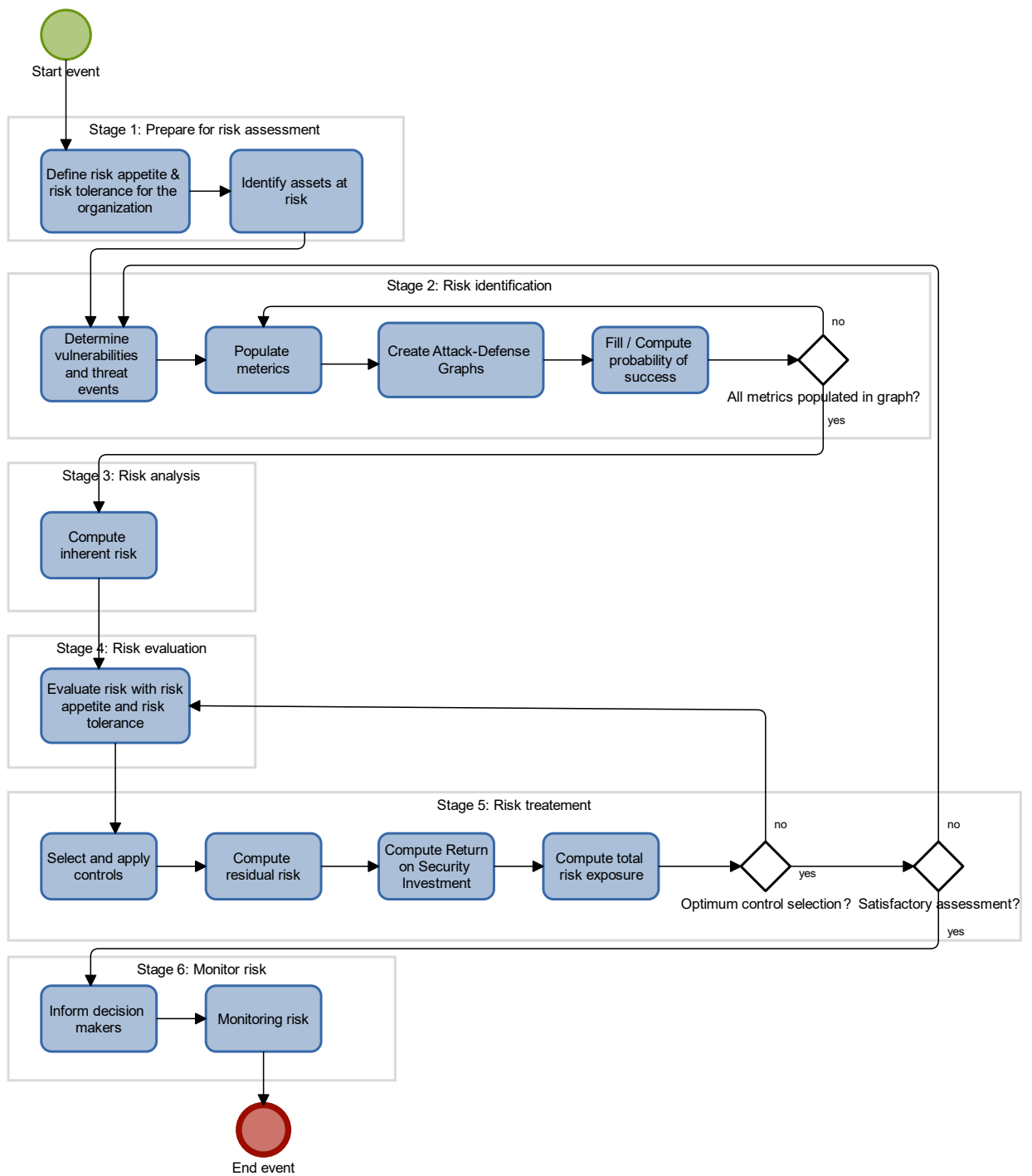


Figure 11 Detailed process diagram for MORSE approach

Stage 1: Prepare for risk assessment

The initial step for organizations is to decide on performing a risk assessment. With that, they must prepare themselves to perform all the steps to ensure a meaningful outcome from the resources that they have committed to. It is expected that the organization already has some form of security and risk expertise before they undertake this assessment. The output of this stage would allow the organization to progress to the next stage of risk assessment.

- Define risk appetite and risk tolerance

Firstly, the organization must define their risk appetite and risk tolerance that would determine how much risk they are willing to take in order to achieve their strategic objectives. As it is an activity that is executed with the involvement of different stakeholders of the organization, it is defined as a motivation view in ArchiMate, as shown in Figure 12 for the example scenario. The stakeholders identified for influencing risk appetite and risk tolerance in the example case are shareholders, board of directors, creditors, and regulators. When an organization decides to undertake a risk assessment, the selection of stakeholders would be the input for coming to a value for these metrics.

In MORSE, the following metrics are defined for risk appetite and risk tolerance:

- **Organizational risk tolerance %** - At an organizational level, a percentage is defined based on the value of the asset that they are willing to risk. This is a generic value that would apply to all business processes in the absence that it is explicitly defined. This metric is defined in the organizational role.
- **Process risk tolerance %** - A process-specific risk tolerance is defined so that certain processes can have a divergence from an organizational level. This may be the case when there are some innovations that stakeholders have committed to, which would require taking additional risk. The value of this is set in the next task when the asset is identified.
- **Organizational risk appetite** – This is defined as a currency value that the organization is willing to accept for total risk to their assets. The combination of all risks in the organization should be maintained to a level lower than this value. Further calculations on it are done in the risk evaluation stage.

Table 9 Stage 1 - Define risk appetite and risk tolerance for the organization

Stage 1 – Define risk appetite and risk tolerance			
Inputs	Mechanism	Output	Viewpoint
- Selection of stakeholders	- define goals - drivers - Organization strategy to achieve objectives	- Organization risk appetite - Organization risk tolerance	Motivation view

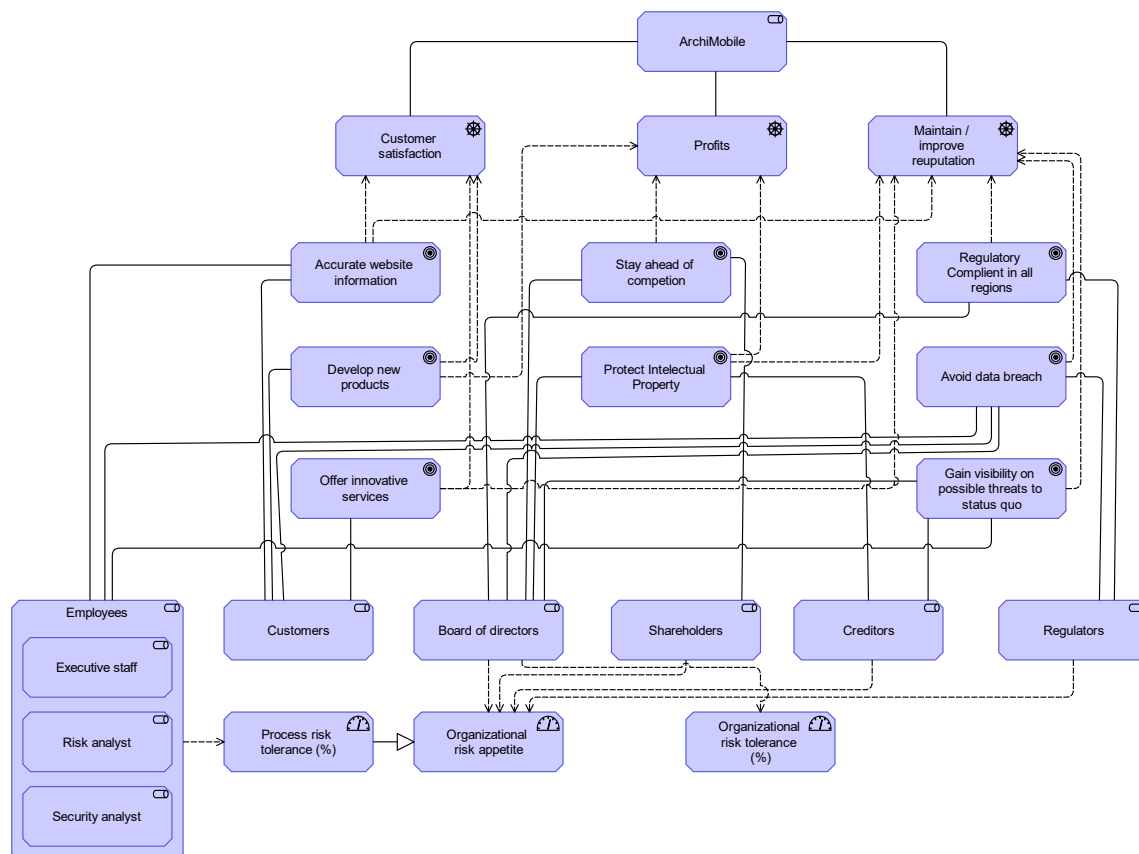


Figure 12 Motivation for risk appetite and risk tolerance

- Identify assets at risk

For the next task, the risk manager has to identify the assets for the risk management process. An asset is anything that is of value to the organization. An asset may be defined in any layer of ArchiMate – Business, Application or Technology. It is expected that a threat actor can cause harm to the organization by compromising the selected asset. Thus, the asset may be, among other things, an information asset, a business process, or an organizational structure that facilitates the normal functioning of the organization.

Identifying them helps in setting the scope and boundary for the risk assessment. This limits what a risk manager would need to focus on while performing the assessment. The asset owner would also be involved in this process and would ideally be able to point out the dependent components which would be affected [54].

For organizations that already have an established Enterprise Architecture model, this would entail selecting elements that should be covered in the risk assessment. Figure 13 (same as Figure 9, placed here for convenience in reading) shows the assets identified in our example scenario – the business processes ‘Adapt public website information’ and ‘Browse public website’. Selecting an asset is an inbuilt functionality in BiZZdesign Enterprise Studio and can be done through properties. Once enabled, a qualitative value for the asset can be provided, however, that is not considered in MORSE. Instead, a value of an asset should be filled as a metric of type Money.

Table 10 Stage 1 - Identify assets at risk

Stage 1 – Identify assets at risk			
Inputs	Mechanism	Output	Viewpoint
- EA model of enterprise - processes, business functions etc.	- Selection of assets based on priority - Limit scope for Risk assessment	- List of assets and related elements - value of the asset - asset owners - Process risk tolerance	Total view

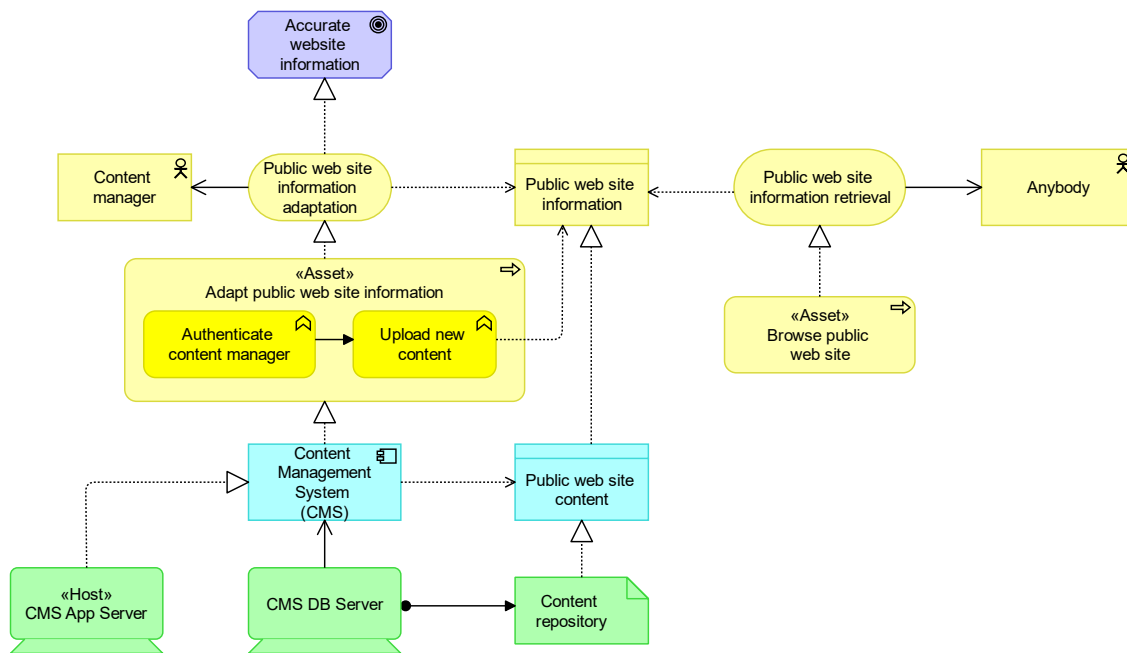


Figure 13 Identifying assets in the model

Stage 2: Risk identification

In the second stage of MORSE, the organization would identify in detail the risk to the assets.

Following the meta-model proposed in the risk and security overlay of ArchiMate [55] (shown in Figure 15), we would use a subset of the concepts. In order to simplify, we only propose to use the following elements in our approach: Risk, Vulnerability, Threat events, Control measure, and Security principle. The risk element is combined with the loss event, so the loss magnitude and loss event frequencies are both associated with it. Additionally, we exclude the threat agent, and that is assumed to be part of the threat event, as the number of times the agent carries out an attack. These relationships are shown in Figure 14.

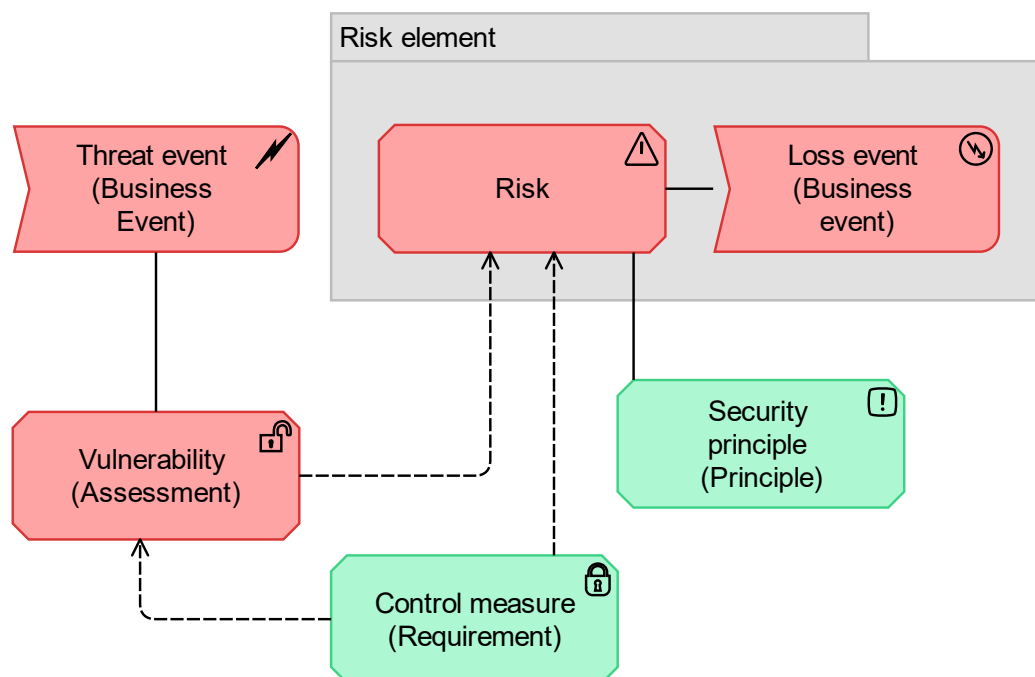


Figure 14 Relationships in the MORSE approach derived from Risk and Security overlay

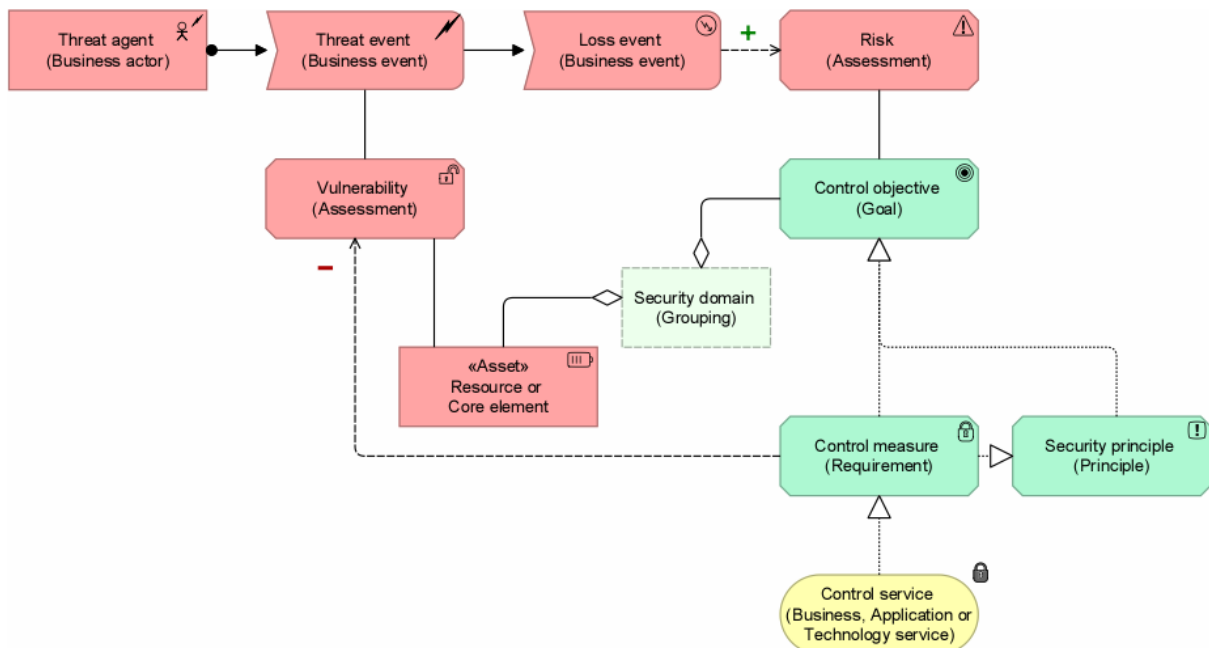


Figure 15 Risk and Security overlay metamodel from BiZZdesign support documents [55]

- Determine vulnerabilities and threat events

The first task in this stage is to define a risk element and identify threats and vulnerabilities to the asset in relation to a loss scenario. For a business element, this would be anything that can impair their proper functioning through a cyber-attack. This includes anything that would impact the Confidentiality, Integrity and Available (CIA) of information relating to that asset. Threats and vulnerabilities are identified in all elements which realize the asset, which means application or technology elements that are essential to recognize the business element would also have to be considered.

For business elements, it is also essential to consider the human factors that can lead to a loss scenario. Emerging attack trends have shown that attackers are targeting unsuspecting employees to gain privileged access to critical systems. Modern security practices take this into account, and vulnerabilities that relate to gaining elevated access through luring employees using social engineering attacks are also modelled during this step.

Applications and technology elements have known vulnerabilities that are available in databases like National Vulnerability Database (NVD) that contain Common Vulnerabilities and Exposures (CVE). However, it should be noted that these only contain publicly known vulnerabilities, and there would be more vulnerabilities within an application or the underlying technology.

Organizations can also use the results of a penetration test, which is performed by vulnerability scanners. These can be directly imported into BiZZdesign Enterprise Studio and create a pool of vulnerabilities relating to their application and technology concepts. Additionally, there may be multiple vulnerabilities in the elements identified from the pen-test, but for relating with the asset, only a few may be necessary. When a need to make such

a choice arises, the threat scenario should be considered, such that only those vulnerabilities that are related to the scenario being modelled are included.

For recognizing the threat events that malicious actors may use, it is also necessary to understand the attack community and their intent related to compromising the asset. Thus, the kind of attack that would be launched by the attacker is also identified in this step.

These vulnerabilities and threat events are modelled in two views. The first view relates them to the business, application, and technology concept in the model. And the second view is for creating the attack graph. Figure 16 shows how this would be modelled in a total view for the running example. The analyst would identify the elements which relate to the asset and model them in this view. Then the risk and security elements are added to it. Please note that control measure elements shown in the figure are added at a later stage, and at this stage, it would only include risk, vulnerabilities, and threat events from the RSO. The next view is the attack defence graph that is created later in this stage.

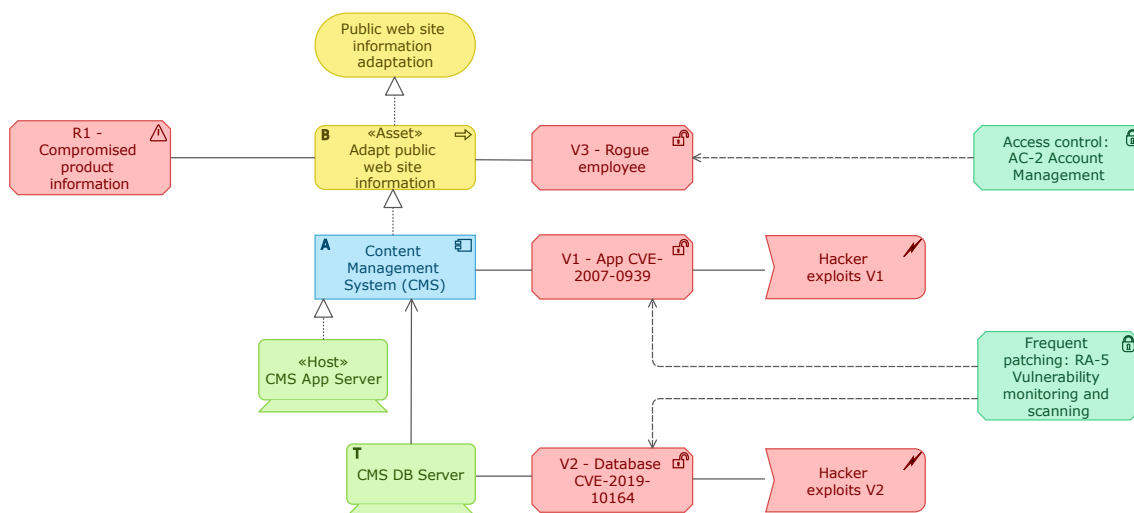


Figure 16 Risk propagation across layers in Attack scenario 1

Table 11 Stage 2 - Determine vulnerabilities and threats

Stage 2 – Determine vulnerabilities and threat events			
Inputs	Mechanism	Output	Viewpoint
- Assets - Supporting elements - applications, technology	- CVE, CWE databases - Known vulnerabilities - Mapping attack surface - Enumerating all possible cyber threats, vulnerabilities, and risks to the asset - Threat intelligence	- Pool of vulnerabilities, threats, and risks	Total view

- [Populate metrics](#)

Based on the literature review performed for this research, we were able to identify many metrics (see Chapter 4). The metrics are units of measurement which can either have a manually inputted value or be calculated based on defined logic. Enterprise Studio defines metrics as a specialization of the ArchiMate driver concept. In this task, the analyst is required to fill in these metrics in the concepts identified. The metrics are explained below.

[Threat Event Frequency](#)

Threat Event Frequency (TEF) is the probable frequency that a threat agent is going to act against an asset in a given timeframe [13]. This is a metric that is defined by FAIR. Within the MORSE approach, the value of TEF is defined for Threat Event elements, and it is estimated for the number of expected attacks in a year. The number can also be a fractional value, as there can be less than one threat in a year, e.g. If there are two threats in 4 years, the TEF for that particular event would be 0.5. Threat Event Frequency is a value that is estimated by the analyst and manually inputted in the model.

The FAIR model additionally defines contact frequency and probability of action for deriving TEF, which have not been considered in our model to limit the number of inputs that are provided by the analyst. FAIR also identifies that it is optional to input all the lower-level values that are in the risk taxonomy abstraction, and an assessment can be carried out by providing just the essential inputs for an effective risk assessment [13]. We would, however, expect that when an analyst is providing input, they have already evaluated the effect of lower-level values according to FAIR, if any.

[Loss Event Frequency](#)

Loss event frequency (LEF) is the number of times that a loss scenario is expected to occur in a given timeframe for a given malicious attack [13]. In our model, the timeframe is defined as a year, and it is called Annual Loss Event Frequency. This metric is derived from the

threat event frequency and need not be filled by the analyst during this phase. The LEF is attached to risk and vulnerability elements.

Loss Magnitude

Loss Magnitude (LM) is the monetary impact in case of a loss event. FAIR segregates LM into two types – Primary Loss and Secondary Loss. Primary loss occurs when the primary stakeholders are affected – the party that bears the loss. Secondary loss is when the secondary stakeholder reacts to the primary stakeholder in case of a loss event. Secondary stakeholders include customer, shareholders, regulators etc. and they may act after the primary loss has occurred. An example for this is when customers move to a competitor after a data breach, because of loss of trust that the company.

For filling metrics, the risk analyst can fill them in these in two variables and the total loss magnitude is the sum of Primary Loss Magnitude and Secondary Risk values. However, for determining these loss magnitudes, the following six forms are defined by FAIR and should be used [56]:

- **“Productivity:** *Loss that results from an operational inability to deliver products or services*
- **Response:** *Loss associated with the costs of managing an event*
- **Replacement:** *Loss that results from an organization having to replace capital assets*
- **Competitive Advantage:** *Losses resulting from intellectual property or other key competitive differentiators that are compromised or damaged*
- **Fines and Judgements:** *Fines or judgments levied against the organization through civil, criminal, or contractual actions*
- **Reputation:** *Loss resulting from an external stakeholder perspective that an organization's value has decreased and/or that its liability has increased”*

Figure 17 shows the relationship between the different forms of losses through a mind-map, as proposed by FAIR and RiskLens. These can be used for evaluating what a particular type of loss can be classified as – Primary or secondary, before giving it as an input to the risk element.



Figure 17 Forms of Losses in Open FAIR, RiskLens via FAIR Institute [56]

CVE/CVSS score

When identifying vulnerabilities earlier in this stage, they can be taken from a vulnerability database to re-use existing known points of attacks. These vulnerabilities are also associated with a score that identifies their severity and this information is provided by the database provider. For CVEs, this value is called a CVSS score.

A pen-test scan can be performed on the environment to find out the vulnerabilities currently present. A functionality is provided in BiZZdesign Enterprise Studio to consume the output of such vulnerability scans. This allows for all vulnerabilities to be available to associate with applications.

Further, additional data can be filled in these vulnerabilities like CVSS score, and this is used to calculate the vulnerability of an element. There have been several researches which focus on performing a risk assessment through CVSS score[57] [58], and our approach uses a formula that is commonly used. The CVSS score is occasionally updated by its maintainers which would change the proposed formula. The one proposed below is based on CVSS version 3.1 which was released in June 2019. It is also valid for CVSS version 3.0.

For deriving the CVSS score, it is a function of exploitability and impact of the vulnerability. Exploitability represents how easy it is to exploit it and impact represents the impact it would have if successfully exploited. The formula for exploitability given in the CVSSv3.1 specifications document [59] is,

$$E = 8.22 * AV * AC * PR * UI \quad (5.1)$$

Where,

- E is Exploitability
- AV is AttackVector
- AC is AttackComplexity
- PR is PrivilegeRequired
- UI is UserInteraction

This exploitability score is defined for CVE vulnerability elements, which may be present in the threat scenario. These can then further be used to derive a probability of success, which is defined further in this stage.

Uncertainty

This metric is defined to factor in the uncertainty in the values that are provided. It is known that risk estimates are hardly ever accurate to exact value. This is because it is hard to precisely predict what the losses would be in case the risk scenario materializes. Thus, it is standard practice to present risk in a range of values. O-RA uses confidence interval along with probability distribution to account for this [33].

We take an uncertainty variable for it. In Enterprise Studio, it is defined as a custom metric type, which allows it to take an enumeration of values. We define this enumeration as *low*, *medium*, and *high*. When filling the values, the analyst would also provide with how much certainty they are giving the values. This metric is populated for the risk element in the scenario. It must be assumed that all elements in the risk scenario would be having the same uncertainty.

Entity relationship diagram

For ease of representation, we developed an entity relation diagram (ERD) which shows what metrics are created in Enterprise Studio. It also shows how the metrics are used within different ArchiMate elements and their relation between each other. The ERD is shown

in Figure 18. The diagram shows all metrics which are in MORSE, including the ones that are computed later in the process.

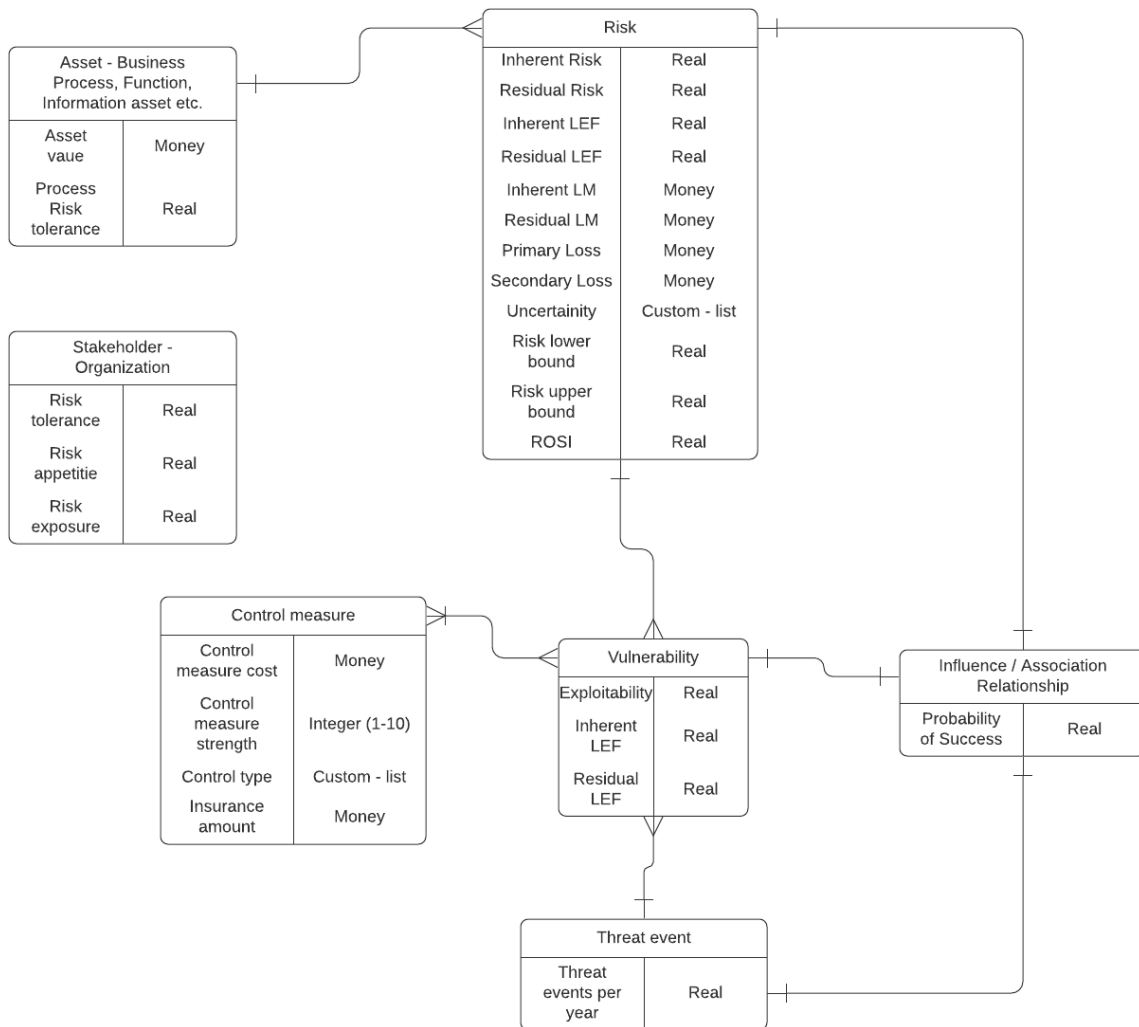


Figure 18 Entity relationship diagram of ArchiMate concepts and custom defined metrics

Table 12 Stage 2 - Populate metrics

Stage 2 – Populate metrics			
Inputs	Mechanism	Output	Viewpoint
- Risk, vulnerabilities, threat events	- Types of losses to the asset - Recent events for calculating number of attacks - CVE databases - Threat intelligence	Metrics: - Number of threats per year - Primary & secondary Loss Magnitude - CVE number - CVSS Score - Exploitability - uncertainty	-

- [Attack-Defence graph & scenario creation](#)

An approach with attack trees is used for the thesis as it allows for modelling the different vulnerabilities that can affect the environment in a graphical form [60]. As stated in the Background chapter, attack trees and attack graphs are a visual method of modelling a sequence of events that lead to a successful compromise of the system. The use of attack graphs is particularly useful as it allows for modelling different ways in which the system can be compromised and what protections can help mitigate the effects. They are predominantly used in security modelling, and in this research, we are combining them with risk assessment.

A 'risk and security view' is created for each risk scenario. In attack defence graphs, the root node can be reached through different attack paths, which are defined as vulnerabilities in our approach. The vulnerabilities are joined in a way that when one is exploited, the attacker can move to the next node and attempt to exploit that. This is called lateral movement within an IT environment. As the vulnerabilities can be linked to a system – technology or application, or a business element, thus the attacker can move in the model through layers in any direction. This means that the attacker may first exploit a business process and then an application component, or it may be the other way around. They can first compromise a system security flaw and go for a business concept. These dependencies are mapped in ADG for the risk scenario.

An analyst would select which vulnerabilities and threat events are related from the catalogue identified earlier in this stage. These are then linked following the convention defined in our approach below. At the end of this task, the analyst would have one or more attack graphs created for a risk scenario.

Risk scenario modelling convention

- One risk element in one view
- One threat event per graph, i.e., each independent threat event would have a separate graph
- On a single view, there may be multiple graphs
- The elements can be joined with AND, OR, or directly with another element
- Threat event is connected to vulnerability through association relationship (from TE to Vuln)
- Vulnerabilities and risks are connected with influence relationship

Figure 19 shows a reference attack graph that is created following the modelling convention.

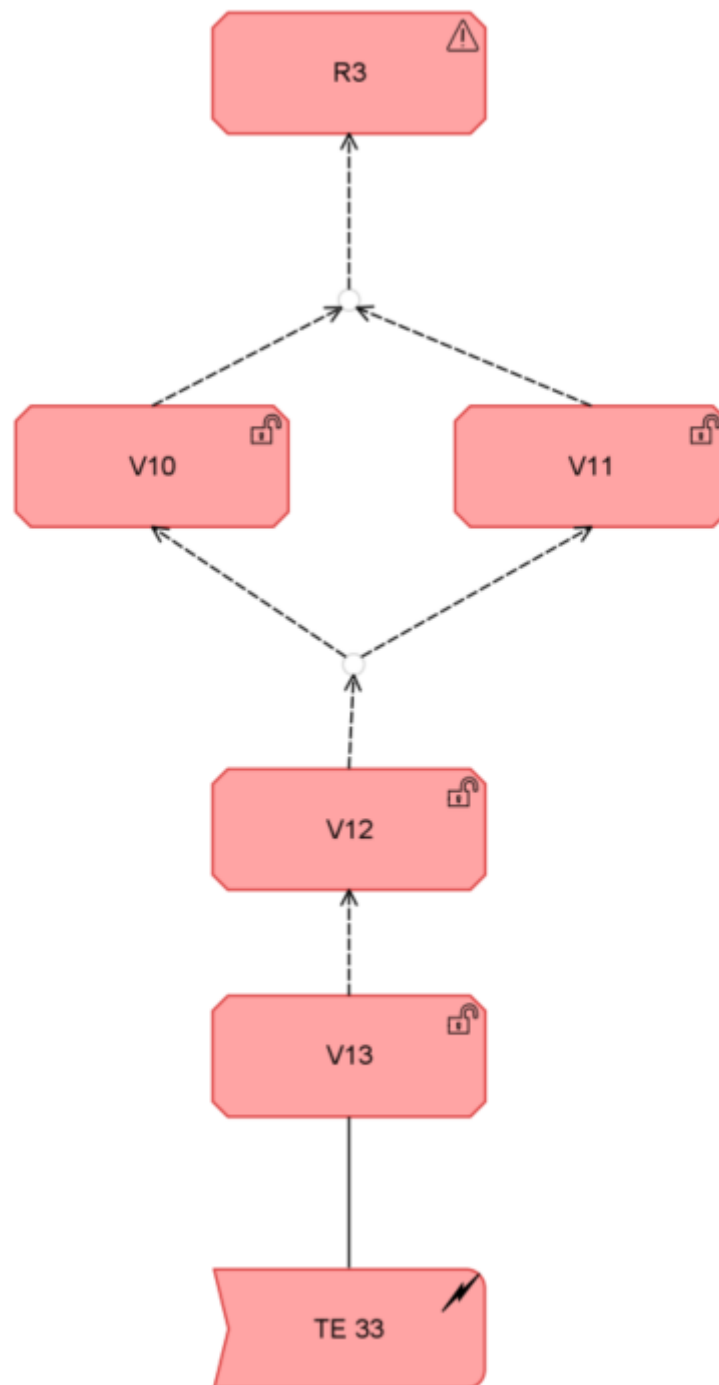


Figure 19 A reference attack graph with various relationships

Figure 20 shows how the risk scenario in the ongoing example would be modelled. Taking R1 as the risk identified, there are two graphs that are created. Each of these graphs has a unique threat event TE1 and TE2, which means that an attacker can take any of the attack paths to compromise the asset. The graphs are then populated with the vulnerabilities V1, V2 and V3 along with Junctions that denote an alternate path that may be exploited. In the left attack graph, it is designed that V2 may be exploited directly by an attacker, or it may

be exploited through V1. This is because the attacker could, in one case, reach the database directly but would have a different probability of success than if they first exploit an application and then using lateral movement within the network reach database to exploit V2. This would have a different probability of success.

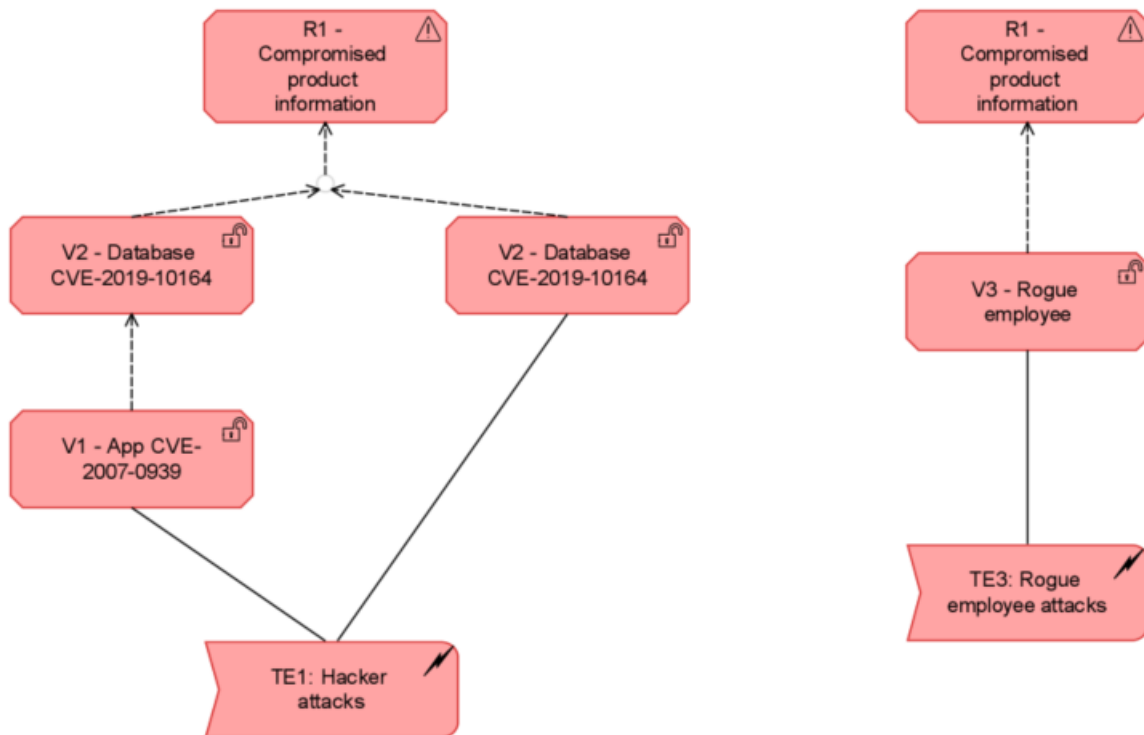


Figure 20 Risk scenario created for Attack scenario 1

Table 13 Stage 2 - Create Attack-Defence graphs

Stage 2 – Create attack defence graphs			
Inputs	Mechanism	Output	Viewpoint
- Risk, vulnerabilities, threat events	- Create risk scenario - Possible attack paths an attacker can take - identify dependencies in reaching target for attacker - Add AND/OR junctions for dependencies - Following modelling convention	- Risk scenario - Attack Graph(s)	- risk and security view

- Fill / Compute probability of success

The probability of success is a metric that is defined in MORSE to estimate how likely an attacker is to compromise a targeted vulnerability. The probability is defined on the relationships in the attack graph and is a decimal value between 0 and 1. A higher probability means that it is easier for an attacker to exploit it and move to the next level node in the attack graph. Similarly, a lower probability means it is a difficult attack to succeed. In the attack graphs, all influence relationships have a probability of success. This probability can be either derived or provided by the analyst.

For estimating the probability of success, a table is created based on perceived ease of exploit. This can be used as a reference by an analyst for filling in values to the attack graph. The values can be different from Table 14 if the probability is estimated to vary.

Table 14 Estimations of Probability of Success for reference

Easy	0.8
Medium	0.5
Hard	0.3

Further, using a CVSS score for technology and application vulnerabilities can be used as a reference. Poolsappasit et al. (2012) [58] define the probability of success as a function of exploitability metric in CVSS base score. However, as there has been an update in the CVSS version, and now it includes an extra parameter for calculation, compared to what was provided when [58] was published. We would thus use a modified formula,

$$p(r) = 1 - (0.256 * \text{exploitability}) \quad (5.2)$$

The constant 0.256 is arrived at as the range of exploitability for a CVE is 0.1- 3.9. This would cover probability in the range of (0,1)

Further, we use the 'AND' and 'OR' junctions to show how two or more elements would combine and propagate in the attack graph. The junctions specify if all the vulnerabilities should be exploited or any. These are based on definitions of AND-decomposition and OR-decomposition used by Poolsappasit et al. (2012) [58]. AND junction means that all the incoming vulnerabilities must be successfully exploited by the attacker to be able to move to the next node in the attack path. OR junction means that if any one of the vulnerabilities is successfully exploited, the attacker can then move ahead.

Figure 22 and Figure 23 show 'AND' and 'OR' junctions are used for connecting multiple elements.

The propagation of probability to the next node is given through the following formulae,

For AND decomposition,

$$p(e) = \prod_{i=1}^n p(e_i) * p(r_i) \quad (5.3)$$

For OR decomposition,

$$p(e) = 1 - \prod_{i=1}^n (1 - p(e_i) * p(r_i)) \quad (5.4)$$

For elements connected to leaf nodes,

$$p(e) = p(r) \quad (5.5)$$

For two elements directly connected (Figure 21),

$$p(e) = p(v) * p(r) \quad (5.6)$$

Where,

$p(e)$ is probability of an element

$p(e_i)$ and $p(v)$ are probabilities of incoming element

$p(r_i)$ is probability of incoming relationship

n is number of incoming relationships

The probability of success on the last element in the attack graph indicate the probability that the loss scenario occurs. Which means that even after the attacker is successful in exploiting all vulnerabilities in the attack path, there are chances that they are not able to inflict damage, thus the attack fails. For example, an attacker is able exploit a database vulnerability that gives them access to sensitive information. However, when they attempt to steal the data, they are detected by SIEM, the SOC quickly blocks them and their attempt fails. This chance of success is captured in the relationship leading from the vulnerability element to the risk element.

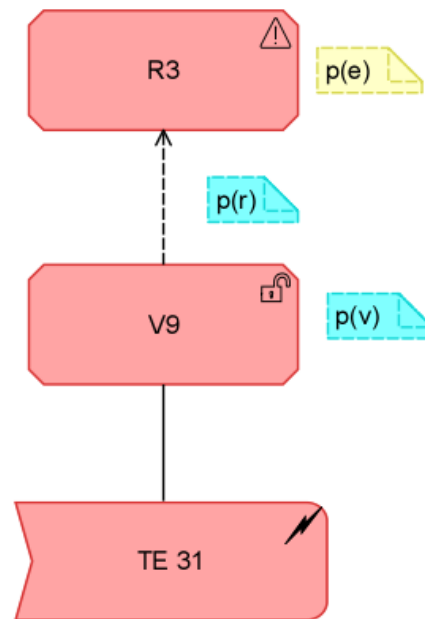


Figure 21 Propagation of Probability of success in simple graph

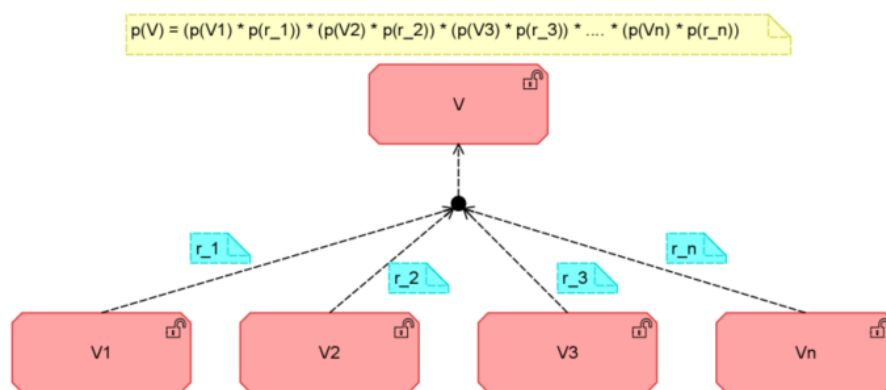


Figure 22 AND decomposition

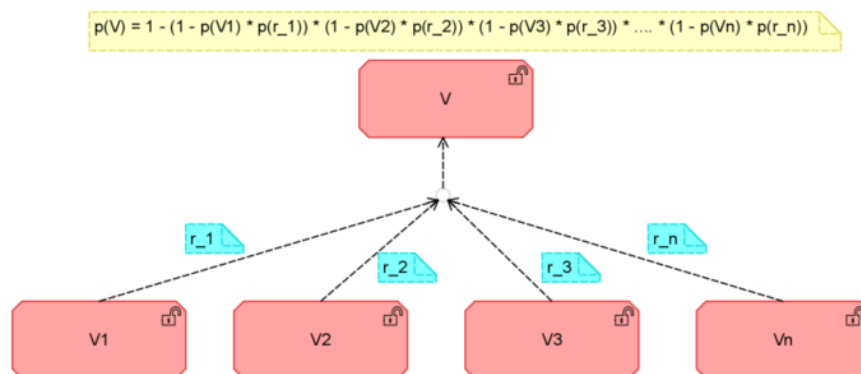


Figure 23 OR decomposition

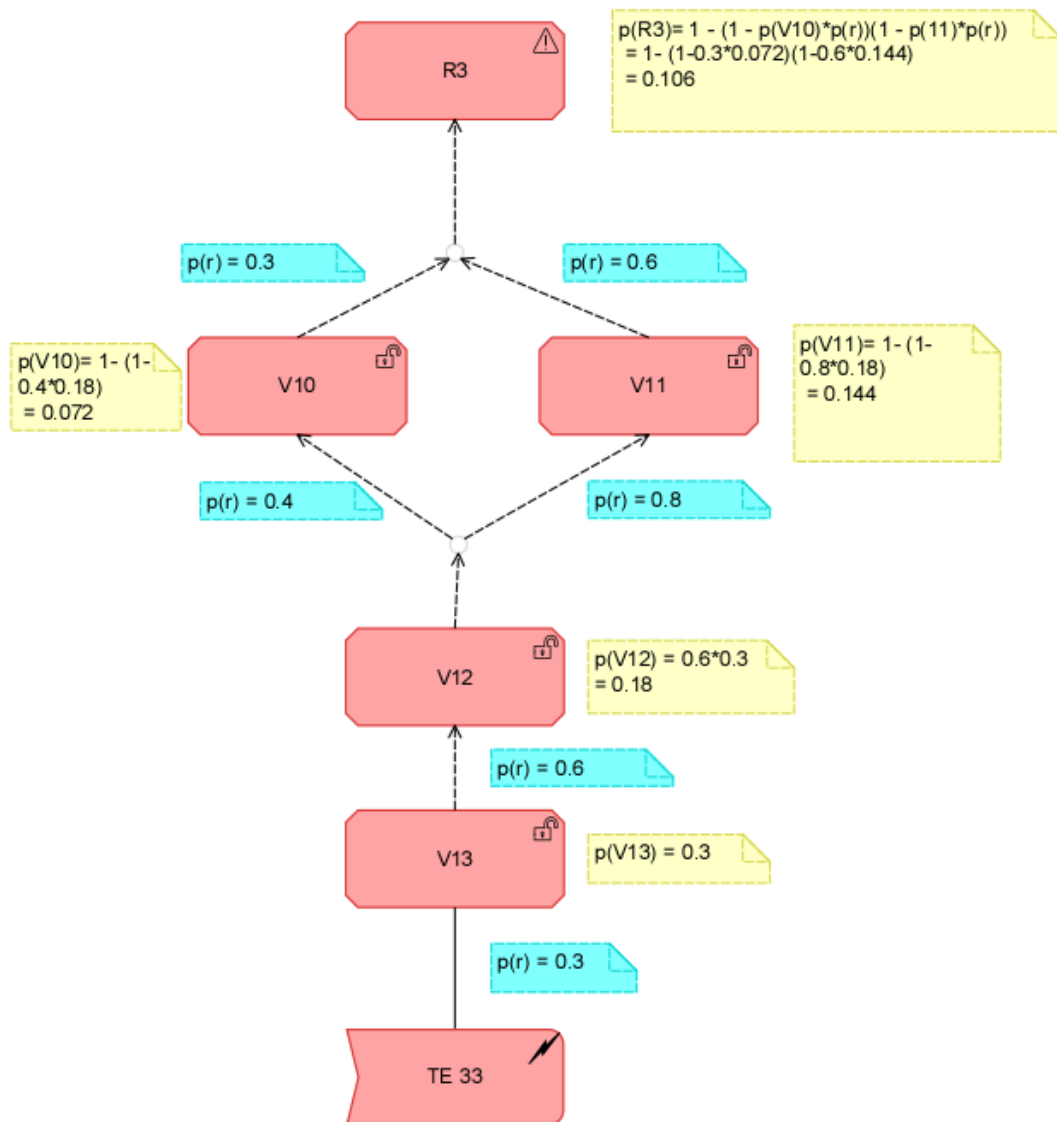


Figure 24 Example of propagation of Probability of Success in an attack graph

Table 15 Fill / compute probabilities of success

Stage 2 – Fill / compute probability of success			
Inputs	Mechanism	Output	Viewpoint
- Attack graphs - Exploitability scores	- using formulae calculate POS - Observe propagation of POS in attack graph	- Probability of success for elements & relationships	- risk and security view

Stage 3: Risk analysis

The next stage in the MORSE approach is risk analysis which lets the enterprise comprehend and determine the level of risk. After gathering all information in the previous stages, a measurement is provided, which the organization can utilize to decide how to best act upon. At the end of this stage, the analyst would have a quantified risk for an asset in the organization.

- Compute inherent risk

The next task is to compute the inherent risk in the risk scenario. Inherent risk is the risk before any countermeasures are taken to protect an asset. For MORSE, this is computed using the industry-standard calculation of risk as a function of frequency and impact. The metrics for risk that are used in our calculations are from FAIR, and they are Loss Event Frequency, Loss Magnitude, and Risk. LM and LEF are defined in stage 2 – Populate metrics, which are derived from Open Fair Risk Taxonomy, as shown in Figure 25. In our calculations, we are going to calculate LM, LEF, and Risk using formulae derived from Open FAIR Risk Analysis 2.0 [33].

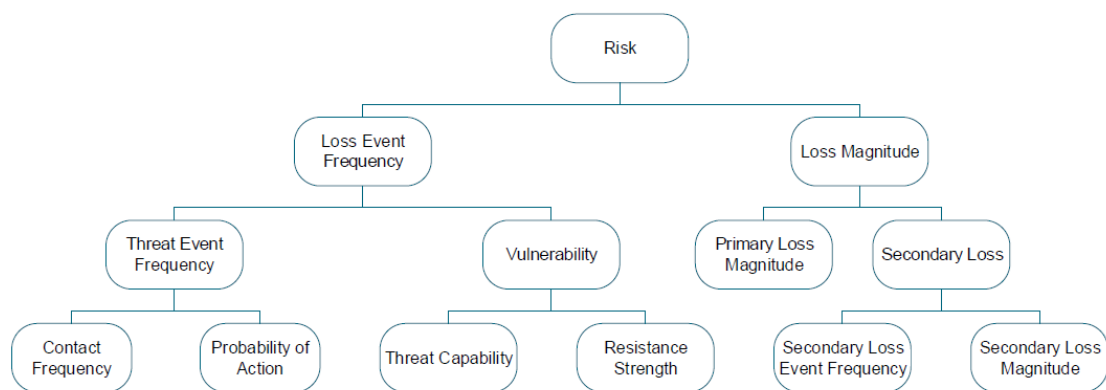


Figure 25 Open FAIR Risk Taxonomy abstraction from O-RT v3 [13]

Loss Event Frequency

The definition of LEF is provided earlier in this report (Stage 2, chapter Design), and here in this stage, LEF is calculated for vulnerability and risk elements. The reason LEF is calculated for both risk and security elements is that there is a frequency at which a vulnerability can be exploited. These depend on the ease of exploitation – measured by exploitability for CVE, CWE type vulnerabilities. These would vary at times and can be lowered by applying controls, such as patching. They are attached to risk element as, one they are necessary for risk calculation, and they also illustrate how many times in a given time period it is likely to occur.

When there are multiple threat events in a risk scenario that would impact a single risk or vulnerability element, then we propose an additional formula (5.7) to be used.

$$LEF_t(e) = TEF_t * p_t(e) \quad (5.7)$$

Where,
t is a threat event

Figure 26 is an example calculation for Loss Event Frequency when there is a single Threat Event. LEF is calculated for Vulnerability V9 and Risk element R3.

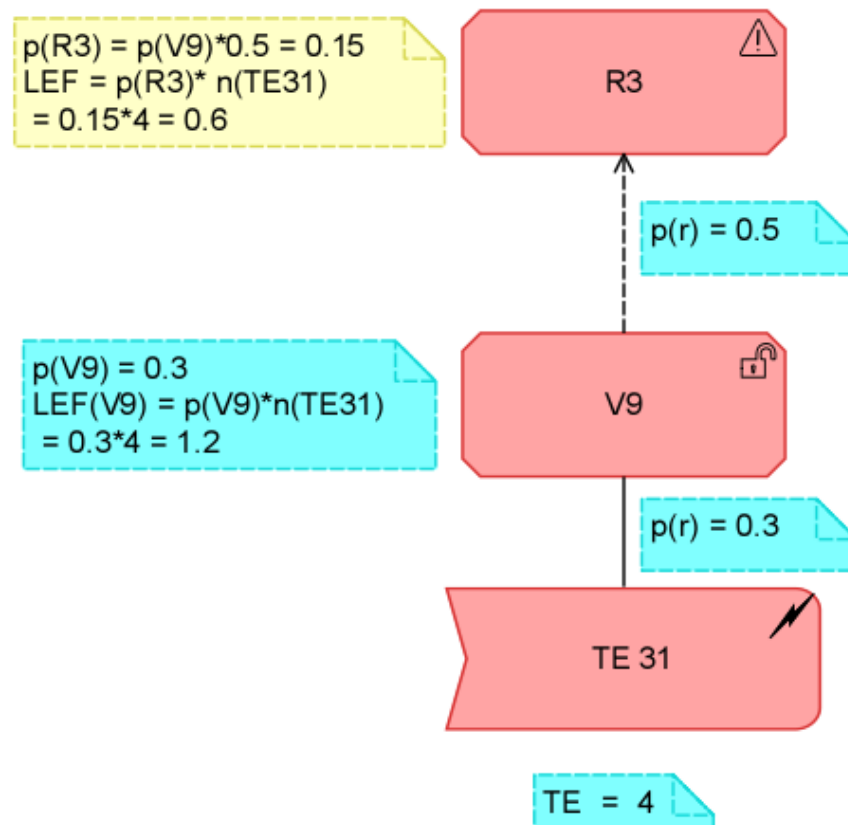


Figure 26 LEF calculation example

$$LEF(e) = \sum_{t \in T} LEF_t(e) \quad (5.8)$$

Where,
T is the set of threat events that can affect that risk/vulnerability in a risk scenario

Figure 27 shows an example calculation for a threat scenario with two threat events. TE31 and TE31 can affect risk R3. Thus, the LEF for R3 is calculated to be the sum of LEF from both of the events. The attack graphs also show the propagation of LEF in the risk scenario. The intermediate steps for calculating the probability of success are not explicitly shown in the figure.

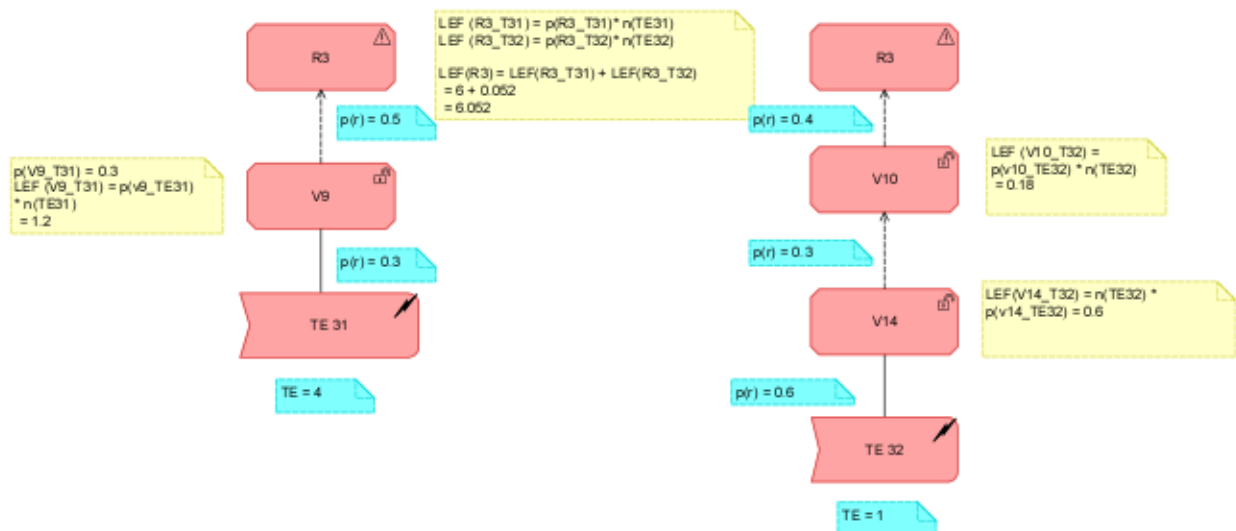


Figure 27 LEF calculation example with multiple threat events

Loss Magnitude

Loss magnitude is calculated only for the risk element. This is the measure of loss in currency terms if a risk scenario materializes.

$$\text{Loss Magnitude} = \text{PLM} + \text{SLM} \quad (5.9)$$

Where,

PLM is primary loss magnitude

SLM is secondary loss magnitude

PLM and SLM are defined for the risk element as per the FAIR standards, and the forms of losses are shown in Figure 17. Primary losses and secondary losses are considered mutually exclusive and exhaustive as defined in FAIR [33] via [29]. For the calculation of SLM, the frequency for Secondary Loss has to be considered when giving the value. It is shown in Figure 25 how the secondary loss is a function of Secondary LM and LEF as per O-RT. In MORSE, Secondary LEF is not taken as a separate input.

Risk

Risk is calculated for only the risk element. The formula for calculating risk is one that is frequently expressed in various forms but largely remains the same. It is a function of the magnitude of impact and the probability of the event happening in a given timeframe.

The unit in which risk can be expressed also varies, but in the MORSE approach, the risk is expressed in terms of currency per year. This is chosen so the risk can be compared based on monetary loss expected in case the scenario occurs. It also removes the need to normalize the value of risk.

As earlier in the approach, we attach the risk element to an asset. It is then known what is the risk for that asset, in terms of money value. A portfolio view is used to tabulate all risk elements in the model. This way, all the risks can be viewed in one place, and if any analysis needs to be done collectively on these risks, they can be performed by a risk analyst. The calculation of risk is given by the following equation,

$$Risk = LEF * LM \quad (5.10)$$

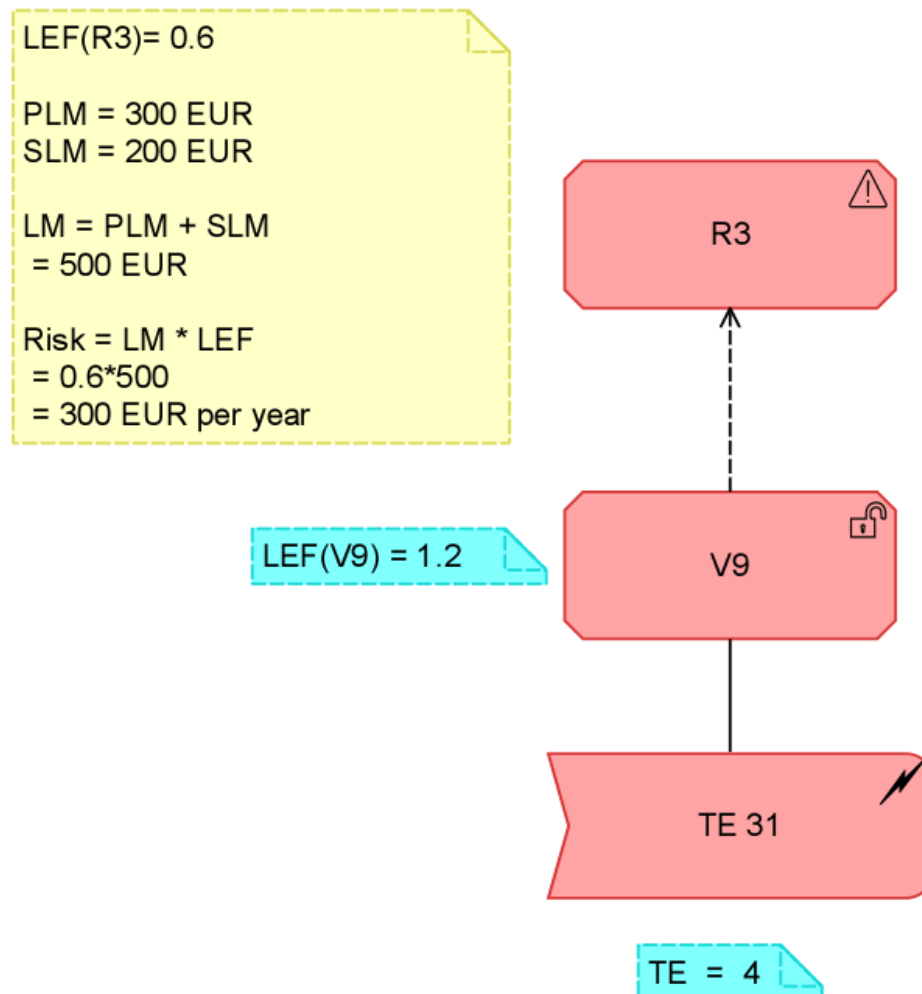


Figure 28 Example risk calculation on attack graph

One drawback here is that the inherent risk is computed considering existing controls that are already in place. These controls/countermeasures may be present internally to the system for protection or additionally added but not modelled in the attack graph.

Post completion of this step, it can also be noted the propagation of LEF values in the architectural model would be available. As there are vulnerabilities attached to the elements in the model, these vulnerabilities would carry the metrics through the model, irrespective of

the viewpoint used. Thus, if we go back to Figure 16, it would correlate to the different values of LEF for the business, application, and technology elements. As already mentioned, we do not compute the risk or loss magnitude value for them.

Table 16 Stage 3 - Compute inherent risk

Stage 3 – Compute inherent risk			
Inputs	Mechanism	Output	Viewpoint
- Vulnerabilities - Risks -Probability of Success	- Compute LEF and LM - Use these values to calculate Risk - Use formulae - (5.7), (5.8), (5.9), (5.10)	- Inherent Risk - LEF, LM	- risk and security view

Stage 4: Risk evaluation

The next stage in the MORSE approach is risk evaluation. Here the risk is evaluated along with other risks in the organization to put them in context, and decisions can be made on how to go further in managing it [54]. Our approach shows what assets would have their risk within the risk appetite and tolerance levels defined.

- Evaluate risk with risk appetite and risk tolerance

In MORSE, there are three metrics related to risk appetite – organizational risk appetite, organizational risk tolerance, and process risk tolerance. These metrics are defined in stage 1 and are used for evaluating the risk of business processes compared to the overall risk in the organization.

Here the residual risk for the asset is used. If the analyst is calculating the risk exposure for the first time for a risk scenario, the residual risk is set as inherent risk, as there are no controls attached to the attack graph yet. However, in subsequent runs, following the process until the risk assessment is satisfactory, the residual risk is updated as controls are added to minimize risk.

Enterprise Studio offers functionality to generate a colour view based on a logic that is defined through scripts. This functionality is utilized here to indicate how the risk of a process is compared to the whole organizations' risk appetite and, in particular, to predefined risk tolerance. To activate risk evaluation task, the analyst would run a script through 'Viewpoints' in Enterprise Studio. We have used colour view because of its intuitive nature that would make this task quick. An analyst can comprehend and communicate at a glance what the result of risk evaluation is by looking at the colours and the legends table.

The following logic is developed for colourizing the assets (limited to business processes in the implementation) within the architecture model,

- PRT = process risk tolerance (%)
 - ORT = Organizational risk tolerance (%)
 - OrgRisk = Sum of all residual risk in the organization (currency)
 - RA = Risk appetite of org (currency)
1. If PRT exists,
 - $RT(\text{Process}) = \text{asset value} * PRT * 0.01$
 2. Else,
 - $RT(\text{Process}) = \text{asset value} * ORT * 0.01$
 3. If Residual Risk (Process) > RT (Process) OR OrgRisk < RA,
 - **Process colour changes to red**
 4. Else if Risk (Process) < RT (Process)
 - **Process colour changes to green**
 5. Else
 - **Process colour changes to blue**

Figure 29 illustrates how this is achieved in the running example case. From the two assets, as we are only performing risk assessment on one, and the risk is within the risk appetite of the organization, it is coloured green. The other asset is coloured blue as it lacks values is not part of the risk assessment. This way, the risk analyst can easily look at the model and conclude which assets need to be investigated.

One edge case in the algorithm is that when Risk (Process) == RT (Process), then also the process would change to colour **Blue**. This was not considered to be incorporated as part of this research to limit the scope, as the number of cases it would happen is small.

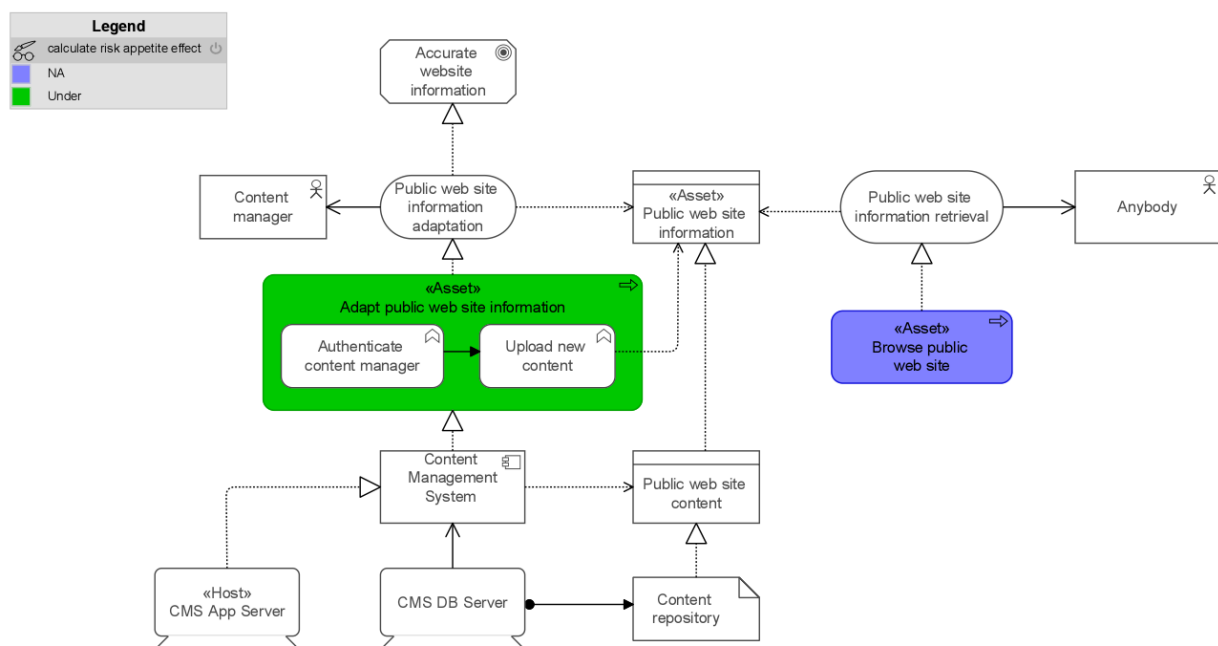


Figure 29 Colour view based on risk appetite

Table 17 Stage 4 - Evaluate risk with risk appetite and risk tolerance

Stage 4 – Evaluate risk with risk appetite and risk tolerance			
Inputs	Mechanism	Output	Viewpoint
<ul style="list-style-type: none"> - Risk appetite - Organization risk tolerance - Process risk tolerance - Asset Risk - Organization risk exposure 	<ul style="list-style-type: none"> - calculated based on an algorithm - Analyst manually runs the script 	<ul style="list-style-type: none"> - Colour view 	<ul style="list-style-type: none"> - Total view

Stage 5: Risk treatment

The next stage in the MORSE approach is risk treatment, where the organization decides which controls to apply in order to reduce the risk to a manageable level. This stage has several tasks, and the goal is to find the optimal set of countermeasures in order to reduce the level of risk.

In this stage, the risk analyst would select appropriate controls for the vulnerabilities in the attack scenario. Considering that the organization has an available SOC that can integrate with the application involved in the risk assessment, there would already be existing controls. In some cases, the SOC may also have multiple security solutions that can be used to mitigate the threat. Furthermore, controls could also be processes that would reduce risk, and as the organization undergoing compliance would have a set of controls like NIST 800-53, ISO27001 etc., standards that would define these. Thus, in this stage, the risk analyst would have to select the optimal controls based on multiple factors.

There are several studies that consider such factors, some of which we encountered during our Systematic Literature Review. On further research, we came across Return on Security Investment (ROSI), in which the goal of the activity is to maximize the gains from the security investments [61, 62]. This takes into account the effectiveness of the control offered and the costs that are involved in order to realize the controls and solve them as an optimization problem. However, in order to limit the scope of this thesis research, we would take a human-centric approach, instead of an algorithmic or math-based approach, to solving the problem. It would rely on the expertise of the SOC personnel and available resources with the organization for the selection of optimal controls. This approach limits the number of controls that can be selected from, as one of the drawbacks of the algorithmic approach is that it returns all possible combinations of controls, disregarding their actual applicability in the attack scenario. It was noted in the study by Muller, Harpes, and Muller (2017) [62], that their case had 7290 possible defence options in their sample case with 81 nodes and 90 defence nodes, out of which not every defence can practically be applied.

Considering that the risk assessment is taken at an organization with an established SOC, the organization would be having a set of controls, which may be based on exiting controls standards such as NIST 800-53, ISO/IEC 27001, CSA or CIS. As part of this research,

BiZZdesign already had a library containing these controls, which was re-used. Further, Gadyatskaya et al. (2016) [61] studied studies across sectors – aviation, finance, and IT, and stated that it is common practice to have a catalogue of countermeasures that can be considered for selection. However, for organizations that are operating in regulated sectors of business, it would be useful to have such a reusable library that can be deployed in models.

For controls in the organizations that can be applied to lower the risk, benefits are analysed such that the maximum returns are obtained. From the popular Gordon-Loeb model for information system investment, the amount that an organization spends on protecting an information asset should not be more than 37% of the expected loss, and in most cases, it should be substantially lower than this value [63].

Next, we describe the activities of the various tasks in this stage.

- *Select and apply controls*

The first task for Stage 5 is to select and apply controls. For the selection of controls for an organization, the risk analyst would have to decide from three options to risk treatment which are explained below,

Risk mitigation

When a risk analyst chooses to apply controls to lessen the risk, it is called risk mitigation. The risk can be mitigated by lowering the probability of a loss event occurring or by lowering the impact of the loss event. An optimal risk mitigation strategy would include selecting controls that provide complete protection of assets and not just bring the residual risk within the organizations' risk appetite. There may be some constraints that the analyst would operate in, which may include budgets, technological limitations or availability of controls in the organization. In MORSE, controls of type 1-4 are for risk mitigation. Control types are described in the following subsection.

Risk transfer

The organization may see the need to transfer the risk to a third party. This may be the case when it is unviable to have controls to completely mitigate the risk. This may be because the loss magnitude is too high for the organization, or in certain regulated sectors, it can be that it is mandatory. The process of risk transfer is done by taking cyber insurance against a given vulnerability. In our approach, this scenario is modelled by creating an additional type of control, type-5 'insurance'.

Risk acceptance

Risk acceptance is when an organization knows the risk but makes an informed decision not to take action to reduce it. This is generally taken as an exceptional case, as it might have implications larger than what is evaluated during the risk assessment phase. It would ideally involve senior management or leadership approval to accept risks. It should also be periodically reviewed if the risk is still acceptable or any other action is taken to reduce the risk.

In MORSE, there is no separate action that would mark a risk as acceptable. However, we would expect that a coloured view of assets would allow viewing if the risk is within the organizations' risk appetite or not. This will let them know if the risk is too high to be accepted or within a bearable level.

Types of controls in MORSE

In this section, we explain the five types of controls available for selection. Control type-1 to type-4 are based on the control categories defined in FAIR, and control type-5 is additionally added. In Enterprise Studio, these are created as metrics with type custom. The type of control is then defined as a metric when filling in metrics associated with that particular control. The calculations related to a reduction in risk are provided after the types of controls. Next, we explain each of the control types.

Avoidance

These types of controls affect the probability/frequency of attack by reducing the number of times the threat agent can come in contact with an asset. These reduce the threat event frequency in the attack scenario. Examples of such controls include firewall filters, relocation of assets, reduction in threat population. Avoidance controls are type 1 controls. In MORSE, these types of controls are to be attached to vulnerability elements and reduce the Loss Event Frequency in the attack scenario.

Deterrent

These types of controls reduce the probability that the attacker would act against the asset. Examples of these controls include policies, logging and monitoring, enforcement practice etc. An example of using such a control would be to include a message that the activities are logged so that potential attackers could be deterred from causing harm, known that they are being tracked. Deterrent controls are type 2 controls. In MORSE, these controls are attached to vulnerability elements, and they reduce the loss event frequency in the attack scenario.

Vulnerability

These types of controls reduce the probability that an attackers' actions would lead to a loss event. These controls focus on increasing the difficulty they would face to compromise a vulnerability. Examples of such controls include authentication, action privileges, patching, some configuration settings etc. In an attack scenario, these could include increasing the strength of authentication by possibly requiring multi-factor authentication for certain applications. Vulnerability controls are type 3 controls. In MORSE, these controls are attached to vulnerability elements, and they reduce the loss event frequency in the attack scenario.

Responsive

Responsive controls are designed to reduce the loss magnitude after a successful attack. These controls are also called Loss Mitigation Controls and support the organization to recover from a Loss Event. Examples of such controls are backup and recovery, incident response processes and forensic capabilities. In an attack scenario, these could be modelled as a response to a successful ransomware attack, maybe to remove the affected machines

from the network to limit the spread of the malware. The process may be initiated as part of incident response and can be either automated through scripts that are triggered or through a network/system engineer who would manually remove machines that are detected to have been compromised. Responsive controls are type 4 controls. In MORSE, these controls are attached to the risk element. They reduce the loss magnitude of a particular risk.

Insurance

This is an additional control type that we add to our classification scheme. With this control, the organization can choose to lower the risk by transferring it to a third party. As there is a growing market for cyber-insurance, many organizations are considering taking insurance to avoid heavy losses associated with cyber risk. It is useful to mark in risk scenario if there already exists insurance or if they would consider to take one for the risk.

The need arises as even with the best controls, there would be cases where the risk would not be lowered to acceptable levels. This leads to the process of risk transfer, which is a broader practice in risk management when the organization takes insurance for a particular type of risk.

The cost metric for this type of control measure is the premium amount that the organization would be paying to be insured. A metric insurance amount is defined for the amount of insurance that is taken. Equation 5.15 gives how this amount is reduced in the risk. Insurance controls are type 5 controls.

Controls of type-2, -3 and -4 can be attached to both risk and vulnerability elements, while type-1 and type 5 controls can only be attached to risk elements. In the next section, we would introduce how these controls would be realized in a SOC environment.

SOC Architecture

For the example scenario, a separate view is created to show the SOC architecture. This represents how the SOC team would design their IT environment to protect the organization. Different applications that are present in ArchiMobile SOC are shown here. They are represented as application components and the services, Nodes for network devices. It also shows the flow of information in the system and how the logs and events from applications are sent to the SIEM system. The output from SIEM is sent to the SOAR system, which selects appropriate responses to the threat. The response is based on the available control measures in the organization. As they invest more in SOC, more capabilities are developed. These are shown in the controls they have to deploy.

A standards-based approach can also be taken by the organization. The controls are available in a portfolio and are from a standard like NIST 800-53. Each control has strength and cost defined. Based on these values, an appropriate control can be taken to minimize the threat from vulnerabilities. It may affect either the loss event frequency or the loss magnitude of an attack. The extent to how much it is reduced is defined by the strength, based on the calculations.

The organizations' SOC contains applications and processes which are used for maintaining the security of the company. It covers the IT and non-IT support required for performing business activities. There are existing measures already in place like SIEM and SOAR solutions which augment the capabilities of the SOC team.

A SOC architecture is prepared in ArchiMate total view and shown in Figure 30. It uses components that are defined in Microsoft Cybersecurity Reference Architectures (MCRA) [64].

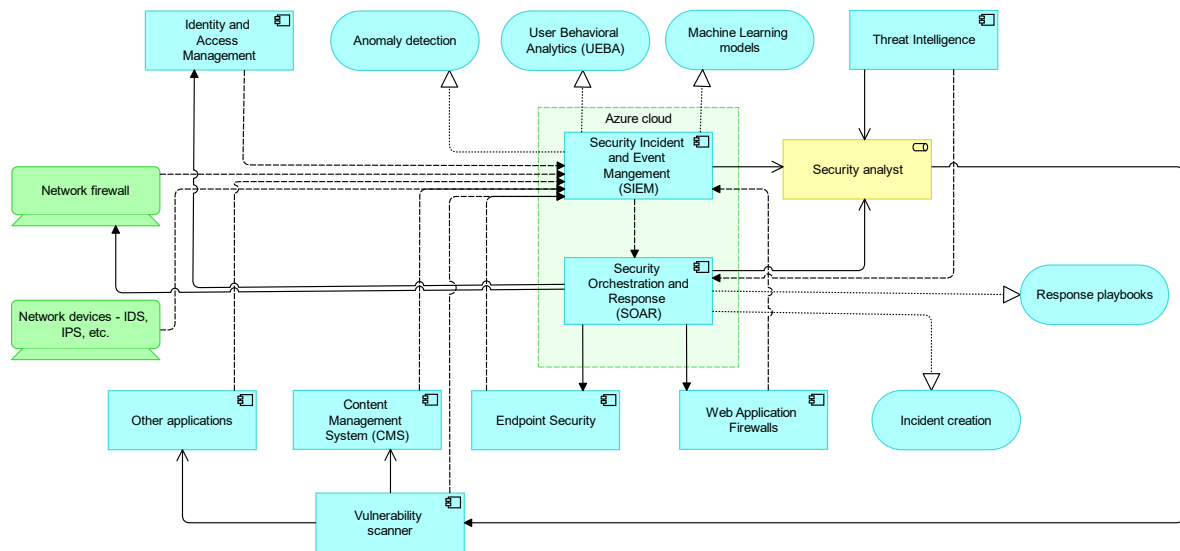


Figure 30 SOC Operations Architecture

Next a new Total view is created to link the applications in the SOC and the controls that are realized by the applications. For the ArchiMobile case, this is shown in Figure 31. For creating this view, the analyst or risk manager would refer to the SOC applications and the catalogue of controls in the organization, possibly from standards. Using the knowledge of what applications offer the functionality to apply the controls, a mapping is created in this view. This view is created because in the attack graph, we are using the control measures to mitigate the risk and through this mapping the analyst can see the applications that can realize that control. They can then check the technical feasibility if it can be used to integrate with vulnerabilities identified in the risk scenario. This task would potentially require additional skills that the risk manager does not have and would involve application SME assistance. The selection of controls in attack graph is explained in the next section.

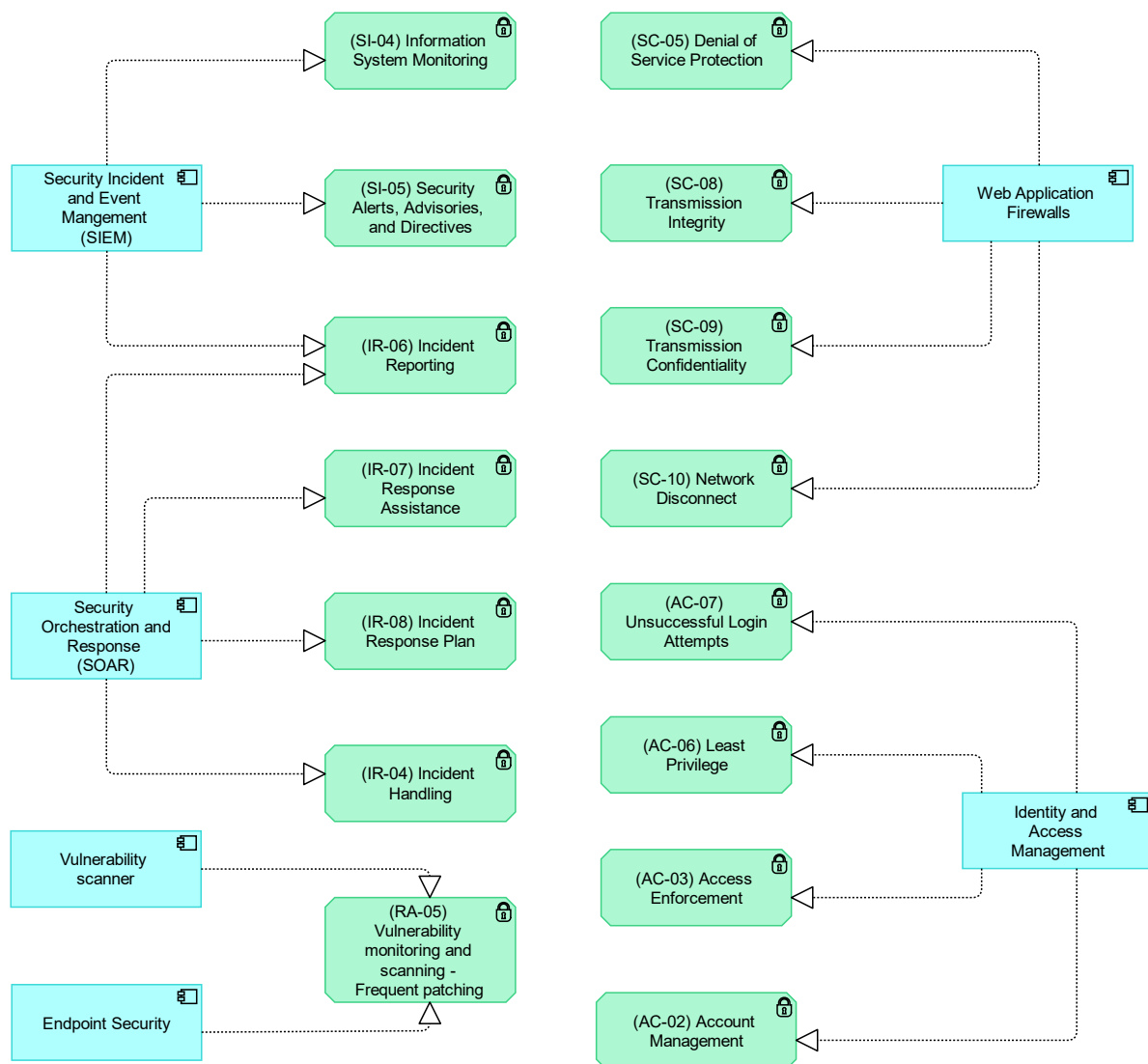


Figure 31 Controls realized from SOC tools

Control measure selection portfolio

In order to effectively manage the large set of controls the organization may be having, we propose using a portfolio for them. The portfolio of controls is managed using the Enterprise Portfolio Management solution in BiZZdesign Enterprise Studio. It provides functionality to manage the entire enterprise landscape – projects, assets, services, capabilities, etc., in portfolios. The process has two phases: design and management. Portfolio design consists of investigating strategy, composing a portfolio and defining valuation criteria for the portfolio. Management consists of populating, scoring and analyzing the portfolio [65].

For selecting controls through our approach, we propose to compose a portfolio of control measures and define the metrics as – control measure cost, control measure strength and control type. Control measure strength is the effective protection that is offered by the

control. As the control is realized through security applications, their strength is defined by the capability of the application to enforce it. We use a scale of 1-10, ranging from weakest to strongest, for measuring the control strength. The value is based on the security analyst's capability to analyse how strong the control measure would be relative to all options available. Control measure cost is also defined for each control. This is the cost it would take to implement the control and maintain it every year. The unit of measurement is EUR per year.

The selection of controls for a given attack scenario is an optimization problem, as stated earlier in this stage. The analyst would select a subset of controls from the portfolio. This kind of approach is studied in literature by [62, 66, 67]. However, in our approach, we would utilize the expertise of the security analyst to look at the ROSI for a subset of control measures in an attack graph and come up with an optimum selection.

Controls portfolio Scorecard	Control measure cost	Control measure strength	Control type
(SC-05) Denial of Service Protection	€ 700.00	7	Avoidance
(RA-05) Vulnerability monitoring and scanning - Frequent patching	€ 200.00	6	Vulnerability
(SC-09) Transmission Confidentiality	€ 400.00	6	Avoidance
(AC-02) Account Management	€ 100.00	8	Deterrent
(AC-06) Least Privilege	€ 600.00	8	Deterrent
(SC-10) Network Disconnect	€ 400.00	5	Responsive - LM
(AC-03) Access Enforcement	€ 600.00	7	Avoidance
(AC-07) Unsuccessful Login Attempts	€ 300.00	4	Avoidance
(SC-08) Transmission Integrity	€ 300.00	4	Avoidance
(IR-04) Incident Handling	€ 700.00	7	Responsive - LM
(SI-05) Security Alerts, Advisories, and Directives	€ 1000.00	7	Avoidance
(IR-08) Incident Response Plan	€ 500.00	6	Responsive - LM
(IR-07) Incident Response Assistance	€ 900.00	8	Responsive - LM
(SI-04) Information System Monitoring	€ 300.00	3	Avoidance
(IR-06) Incident Reporting	€ 800.00	6	Responsive - LM

Figure 32 Portfolio scorecard of controls

Table 18 Stage 5 - Select and apply controls

Stage 5 – Select and apply controls			
Inputs	Mechanism	Output	Viewpoint
<ul style="list-style-type: none"> - Attack scenario risk and vulnerabilities - Control portfolio 	<ul style="list-style-type: none"> - Select controls from available catalogue - Optimize return on security Investment by selecting controls 	<ul style="list-style-type: none"> - Attack defence graph 	<ul style="list-style-type: none"> - Risk and security view

- Compute Residual risk

Once the controls are added to the attack graph, the next task is to calculate their effects and compute the residual risk.

For controls of type 1, their effect is calculated according to the following formula

$$\text{Residual LM} = (10 - CS) * 0.1 * (LM) \quad (5.11)$$

For controls of type-2, -3 and -4, the residual LEF is calculated as per the following formulae,

$$\text{Residual } p_t(e) = (10 - CS) * 0.1 * p_t(e) \quad (5.12)$$

$$\text{Residual } LEF_t(e) = TEF_t * \text{residual } p_t(e)$$

$$\text{Residual } LEF(e) = \sum_{t \in T} \text{Residual } LEF_t(e) \quad (5.13)$$

Here,

e is the element – Risk or Vulnerability

T is a set of all threat events related to e in an attack graph

The residual probability of success is calculated as that is used in the propagation within the attack graph. These follow the same convention as given in the ‘AND’ and ‘OR’ decomposition in stage 2. A known limitation for this method would be that LEF is calculated as an aggregate when there are multiple attack graphs with the same element. However, we choose to keep it as such to reduce complexity in calculations.

Next, we calculate the residual risk after all controls have been selected in a risk scenario,

$$\text{Residual risk} = \text{Residual LEF} * \text{Residual LM} \quad (5.14)$$

The formula that is used to calculate the resultant risk when insurance control measure is also added is given below,

$$\begin{aligned} \text{Residual risk (with Insurance)} \\ = \text{Residual risk} - \text{Insurance amount} \end{aligned} \quad (5.15)$$

The next thing that we calculate is the range in risk. Even though we have arrived at risk values, in practice, it is next to impossible to estimate that the risk would be an exact value. Thus, we calculate a range in which the estimated risk should fall. We propose to use the uncertainty in values collected to arrive at a final risk range. The Uncertainty metric is filled by an analyst in earlier stages and used here to arrive at a lower bound and upper bound for the residual risk.

$$\text{Risk lower bound} = \text{Residual risk} * (1 - \text{uncertainty}) \quad (5.16)$$

$$\text{Risk upper bound} = \text{Residual risk} * (1 + \text{uncertainty}) \quad (5.17)$$

Where,

$$\text{uncertainty} = \begin{cases} 0.05 ; \text{low} \\ 0.15 ; \text{med} \\ 0.30 ; \text{high} \end{cases}$$

Table 19 Stage 5 - Compute residual risk

Stage 5 – Compute residual risk			
Inputs	Mechanism	Output	Viewpoint
- Attack defence graph - LEF, LM, Risk - Uncertainty	- proposed formulae for residual LEF, LM and risk calculations	- Residual LEF, LM - Residual risk - Risk range	- Risk and security view

- Calculate the return on security investment

This task is performed while selecting the controls to mitigate the risk scenario. A ROSI (Return on Security Investment) is calculated for each arriving at a cost-benefit analysis in the risk scenario. It takes into account the benefits offered by security investment. The net benefits are calculated as the reduced risk and the cost of applying the controls. The cost is the sum of all the controls in the particular attack scenario. The following formula for calculating ROSI is arrived at based on [62] and [61] mentioned in the beginning of this stage.

$$\text{ROSI} = \text{Inherent risk} - \text{Residual risk} - \text{Control cost} \quad (5.18)$$

Where,

Inherent risk and Residual risk are same as calculated earlier
Control cost is sum of all controls in the risk scenario

In the risk scenario view, the ROSI is displayed and refreshed through a script. Thus, every time a new control is added to the graph, the value can be updated to see its effects and the analyst can decide if it is more efficient to include it or switch to other controls.

Sonnenreich, Albanese, and Stout (2006) [68] state that the accurate value of ROSI is not as important as a measurement that is consistent and repeatable. The values of ROSI calculated through our proposed formula can thus be used to compare different attack scenarios on how efficient the control measure selection is.

Table 20 Stage 5 - Compute Return on Security Investment

Stage 5 – Compute return on security investment			
Inputs	Mechanism	Output	Viewpoint
- Inherent risk - residual risk - cost of controls in risk scenario	- using formula calculate ROSI	- Return on security investment	- Risk and security view

- Compute total risk exposure

The next task is to measure the total risk for the organization and how the current risk would add up to it. This way, the analyst would be able to see how the existing risk to the organization relates to the current scenario.

Here an assumption is made that all the risk events are independent, else it would cause an error in calculations for the organizational risk exposure. Independent risk events mean that the effects of one event are only considered once. If a threat event leads to two risks, then they must be separated in such a way that the events are independent for individual risk scenarios. This can be done by limiting the scope for each of the risk scenarios. This way the risk exposure is calculated as the sum of risk on all the assets in the model. The formula for calculating risk exposure is given below.

$$Risk\ Exposure = \sum_{a \in A} (Residual\ Risk)_a \quad (5.19)$$

Where,

A is the set of all assets included in risk assessment

Table 21 Stage 6 - Compute total risk exposure

Stage 5 – Compute total risk exposure			
Inputs	Mechanism	Output	Viewpoint
- Residual risk of all elements in organization	- Sum of all risks to the organization's assets - Analyst uses scripts to calculate	- Risk exposure	- Motivation view

Stage 6: Monitor risk

The last stage of the MORSE approach is a continuous process once the initial assessment has been performed. It is expected that there would be continuous updates in the threat landscape for any organization as time progresses. There are two tasks in this stage – inform decision-makers and monitoring risk.

- Inform decision-makers

The leadership and executive decision-makers in the organization should be periodically informed about risks to the organization. They can communicate it further to the stakeholders who influence the strategy for the organization and thus can make appropriate decisions in line with a long-term view. They can be informed through reporting risk in the form of periodic reports – monthly, quarterly or annual. These reports should contain all appropriate information about how effectively the risk management strategy is working.

Following a report by McKinsey highlight the need for executives to be aware of how critical assets are protected for making informed decisions about countermeasures [69]. Miscommunication often leads to overprotecting low-priority assets and under protecting critical ones. They propose, and we concur, that cyber risk reporting should consist of three fundamental objectives

- **Transparency on cyber risk** – The report should include transparent information on the most valuable assets for the organization, with data of the most dangerous threats and important defences assembled.
- **Risk-based enterprise overview** – providing a risk-based overview of the enterprise so decision-makers can focus on cyber security investments to mitigate the most dangerous threats from attacking their valuable assets.
- **Return on cyber investment** – ensuring a high return on investment by efficiently selecting countermeasures.

These should be included in the report circulated to decision-makers which are worded in such a way that they can understand. The reporting should avoid giving technical terms like applications, servers and technology, replacing them with the quantified business impact expected from the loss of assets.

Thus, for MORSE we propose to create reports which can serve different audience and be consistent in their reporting. In Enterprise Studio this is done by the use of dashboards, where charts and tables can be added. We recommend having the metrics of Risk, Residual risk, Risk range, LEF, LM, Risk appetite, Risk Tolerance and Risk exposure at minimum. This would vary depending on organizational needs. A sample risk report is given in the next chapter, Demonstration. The report can also be shared in different formats as not all the stakeholders would be users of a software, and PDF or HTML file format is the most compatible for reporting.

Table 22 Stage 6 - Inform decision makers

Stage 6 – Inform decision makers			
Inputs	Mechanism	Output	Viewpoint
- Results of the risk assessment - Selection of Stakeholders to inform	- translating results to effectively communicate with stakeholders - Highlighting actions/decisions to be taken by them	- Risk report	-

- [Monitoring risk](#)

The last task is monitoring risk in the MORSE approach. For the risk to the organization, the LEF would change based on the vulnerability – if it becomes easier to exploit it, or the organization buys new applications to improve their security posture.

The CVSS score of security vulnerabilities also changes over time. We are, however, only using the base metric and particularly exploitability which does not change over time. However, there are temporal aspects to the score as well. We would propose that in an implementation of this approach, it is extended with programmatically updating the CVSS score. This can be done through APIs. Red Hat provides Security Data APIs ([Product Documentation for Red Hat Security Data API 1.0 – Red Hat Customer Portal](#)), which allow to retrieval of CVRF, CVE and OVAL data easily and without authentication. Combining this with BiZZdesign Open API, it can be used data enrichment in the architecture model. However, as part of this research, this aspect was not tested in the model and is proposed an enhancement to automate parts of the process.

The organization is also expected to evolve over time which would influence a change in other metric values proposed in this approach. The loss magnitude for a process may also change over time when the business expects higher losses if the processes are affected. When the asset value increases or decreases, the risk must be suitable adjusted to provide an accurate picture.

Further linking it with an automated SOC, an up-to-date risk assessment of the environment would provide a picture of coverage of the defences in place. When there are new applications concepts added to the architecture, they would also require to be integrated into the SOC landscape, and overall risk exposure of the organization would be beneficial.

Periodic risk assessment for the organization to factor in new tools that are added to the SOC. This would allow improved security for existing applications and processes, but an analyst would have to modify existing attack scenarios to see their applicability. This in the MORSE approach we propose that an organization chooses the frequency with which they perform a periodic risk assessment.

Table 23 Stage 6 - Monitoring risk

Stage 6 – Monitoring risk			
Inputs	Mechanism	Output	Viewpoint
<ul style="list-style-type: none"> - Assets for risk assessment - Existing risk scenarios - Any changes in organization strategy 	<ul style="list-style-type: none"> - Threat intelligence - Vendor security updates - Other sources which update threat landscape for the enterprise IT 	<ul style="list-style-type: none"> - Update risk scenarios in the model - Update Risk appetite, risk tolerance - Periodic risk assessment frequency 	-

5.3. Comparison with ERSM process

In this section, we compare the proposed approach with the ERSM process, which was introduced in the Background chapter. This comparison is made using information retrieved from BiZZdesign support documents [55] and Jonkers and Quartel (2016) [14].

The major difference is that ERSM is a qualitative risk assessment process, while MORSE is quantitative. In order to achieve this, we go with a creating attack graph where we show how risk can propagate in an EA model. ERSM has two main phases, risk assessment and security deployment, and these have nine steps. While MORSE has six stages and fourteen different tasks, in addition to 3 decision nodes which introduce feedback loops in the process.

MORSE uses a subset of elements (see Figure 14) from the ERSM relationship model (see Figure 15). In MORSE, we combine the risk element with loss event element, so it is always associated with a loss scenario. However, in ERSM, a risk can have a loss or not which are presented in a separate Loss Event element.

ERSM implementation in Enterprise Studio uses 4-6 levels of ordinal traffic lights and colour view to display the values and heat maps to visualize quantitative risk analysis. MORSE utilizes colour view for risk evaluation, and portfolio scorecard view to display the numeric output of the analysis.

We further list out some similarities and differences in Table 24 below.

Table 24 Comparison of MORSE with ERSM

	Similar in MORSE and ERSM	Different in MORSE Approach
Risk assessment	<ul style="list-style-type: none"> - Selection of risk, vulnerabilities and threat events - Vulnerabilities are linked with EA model elements - Based on Open FAIR Identification of assets - Identification of assets 	<ul style="list-style-type: none"> - Quantitative process - No separate loss event element - Order in which they are done – we propose to define risk first, then vulnerabilities and threat events. - Creation of risk scenarios - Attack graphs, propagation of risk in the attack scenario - Cause and effect of exploiting one vulnerability to affect another one - Evaluation of risk appetite for process and organization
Security Deployment	<ul style="list-style-type: none"> - Selection of control measures 	<ul style="list-style-type: none"> - Addition of control measure nodes to the attack graph - Not all security deployment elements used in our proposed approach – restricted to control measure and security principle - Selection based on a portfolio strategy

5.4. Conclusion

To conclude our design here, we have proposed a quantitative risk assessment technique that has six stages. The stages are in line with the industry standards – preparing for assessment, risk identification, risk analysis, risk evaluation, risk treatment and monitoring risk.

Once an organization decides to perform a risk assessment, in the first stage, they would define their risk appetite and risk tolerance in line with stakeholder desires. They would also have to decide what asset to perform the risk assessment on. In the second stage, the threats and vulnerabilities are identified. Risk scenario is created by using attack graphs, and all metrics are populated based on estimations and CVE databases. In the third stage, risk analysis is performed where the LEF, LM and risk value are calculated. In the fourth stage, the risk is evaluated with the risk appetite and risk tolerance and shown to the user using a colour view. In the fifth stage, control measures are selected to reduce the risk exposure of the organization. We have proposed a portfolio-based approach in which an organization's available controls are displayed on a scorecard. The analyst would select the appropriate controls in order to optimize the return on security investment by applying these controls. In the sixth stage, the relevant stakeholders are informed, and any updates to the risk scenario are performed periodically.

The next chapter would show a demonstration of the MORSE approach applied to another attack scenario to illustrate how it is intended to be used.

6. Demonstration

The next step in the engineering cycle from the Design Science Methodology by Wieringa (2014) [6] is treatment validation which we cover in this chapter. The treatment validation is performed on a model of the artefact in a model context. For this research, we would be doing that through a demonstration of the model. It will walk through the stages an IT risk manager or analyst would be performing to use the proposed design. Finally, we assess the requirements initially identified, if they are satisfied and to what extent. Peffers et al. (2007) [20] enumerate this step as 'Demonstration', which is carried out after 'Design & Development' in their DSM.

In this chapter, we use the same business scenario that is defined in the earlier chapter and develop an alternate risk scenario. This way, we also demonstrate how multiple attack scenarios can be modelled by an organization using the MORSE approach. The demonstration is shown in BiZZdesign Enterprise Studio as with the rest of the development. In the images, blue comments depict values that the users input and yellow comments depict values that are calculated.

In the next chapter, we describe a mini-workshop that was conducted in which the sample case was demonstrated to the participants. At the end of the workshop, the participants were asked to fill an evaluation form. The responses from the evaluation form are used in the Evaluation chapter of this thesis. The workshop also included a presentation in which the participants were introduced to the MORSE approach. During the demonstration, we went through each of the stages. The sections below show steps that were part of the demonstration during the workshop, along with additional explanations.

It should be noted that Attack scenario 1 mentioned in the Design chapter was shown in the mini-workshop instead of the one below. Attack scenario 2 was prepared for a hands-on exercise to be performed during the workshop, however, due to the limited time, it was decided to discuss the MORSE approach amongst participants instead of the hands-on exercise.

Attack scenario 2

An employee receives a phishing email that contains a malware attachment. As there are no spam filters/virus scanners in their mailbox, it is undetected. The employee opens the attachment, which encrypts their system. The malware quickly spreads in the network, and computers in the local network are rendered unusable. The data on their local storage is encrypted, and the attackers now ask the organization to pay a ransom to decrypt their data.

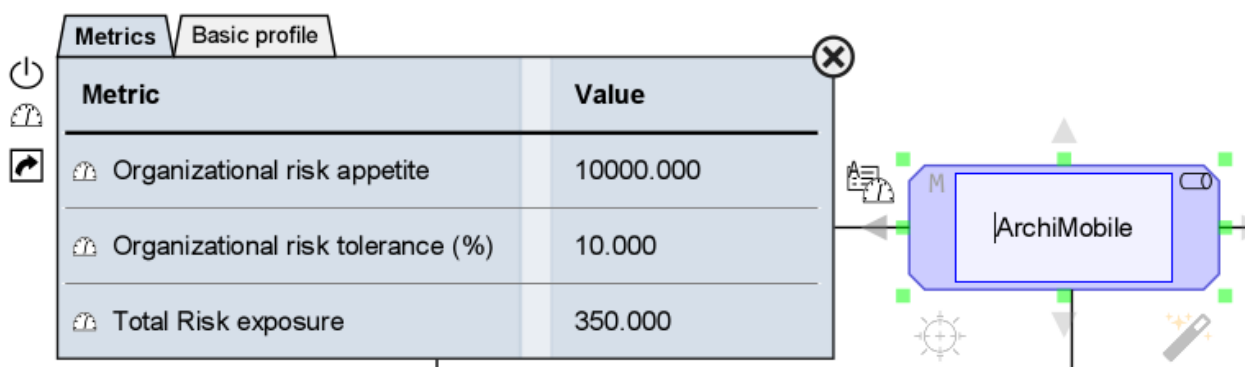
The employees who are affected belong to the finance and administration teams. Fortunately, not all the people are in the same location/network, and some of the work can be carried on by the remaining team. However, productivity is impacted, which leads to fewer orders being processed because of this attack. To contain the impact, everyone in the office is asked to disconnect their systems from the network.

The primary loss magnitude in this attack is estimated at EUR 10,000.

6.1. Stage 1 – Prepare for risk assessment

- Define risk appetite and risk tolerance

The first task in MORSE is preparing to perform a risk assessment by defining the risk appetite and the risk tolerance at organizational level. The input in this task is the selection of stakeholders that influence these values. In the example case, these are Board directors, Shareholders, Creditors, and Regulators for Organizational risk appetite, and Board directors for Organizational Risk tolerance (%). The values of these metrics are derived from the goals and strategy of the organization. For ArchiMobile, the drivers are customer satisfaction, Profits and to maintain/improve the reputation of the company. Based on these goals are defined which are related to each of the stakeholders. Considering the market presence of ArchiMobile, the stakeholders have decided to set Organizational risk appetite as 10.000 EUR and Organizational risk tolerance as 10%. These are displayed in Figure 33, and the motivation view is in the previous chapter, Figure 12. Metrics are selected in the tight pane for the element properties. Add each metric by selecting from the list after clicking the 'Add metric' button



Metric	Value
Organizational risk appetite	10000.000
Organizational risk tolerance (%)	10.000
Total Risk exposure	350.000

The screenshot shows a software interface with a 'Metrics' tab and a 'Basic profile' sub-tab. The table above displays the data for these metrics. To the right of the table is a diagram of the 'ArchiMobile' organization model, represented as a blue rounded rectangle with various icons and connections around it.

Figure 33 Organizational Risk appetite and Risk tolerance set

- Identify assets at risk

The next task is to identify assets for the risk assessment in the enterprise architecture model for ArchiMobile. Considering that the organization uses EA models, we create a total view using existing elements and adding new ones as needed for this viewpoint. Then assets that are affected by the threat scenario are identified. In this attack scenario, 'Order processing' process is marked as an asset. Figure 34 shows this view.

The figure shows how the 'Order processing' process is realized by application and technology components. These are further used in the risk assessment process as any effect on them would also impair the ability of the organization to function adequately. As mentioned in Attack scenario 2, the finance team is affected because of the ransomware attack on the PC of an employee, and thus we include them in risk assessment. These are not marked as assets in this step as the risk is measured at a higher layer, i.e. the business process is impacted by the attack. We consider their impact during the risk assessment.

In this step, we also have to set the 'value of asset' and the 'process risk tolerance'. This task is done in consultation with the process owner. Here we set the 'value of asset' as EUR 1.000.000. The process risk tolerance is left unset, which means that the organizational value is considered.

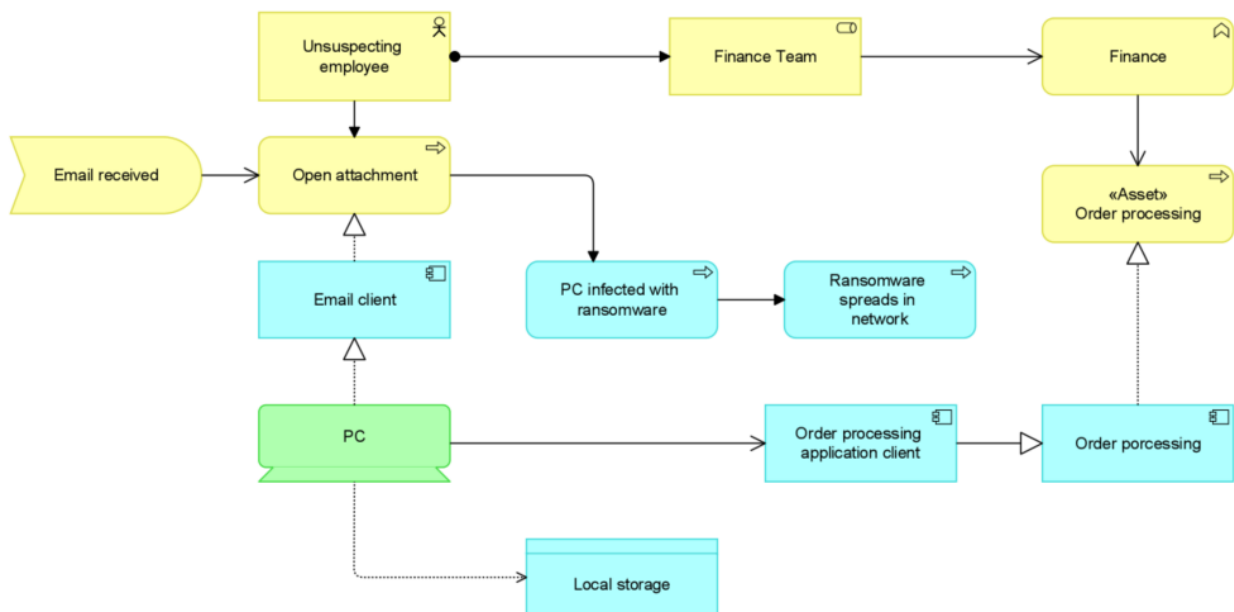


Figure 34 Total view attack scenario 2

6.2. Stage 2 – Risk identification

- Determine vulnerabilities and threats

In the next task, the risks, vulnerabilities and threats are identified for the asset 'Order processing'. This is done first by identifying the related application and technology elements in the model. A new view is created using the elements in the total view, which is used for modelling threats and vulnerabilities across different layers. Figure 35 shows how this looks after identifying these in the model.

For this case, one risk is identified, three vulnerabilities and one threat event. These are all linked to different layers. R4 is the risk that is identified in the business process, which is 'Inaccessible order data' that the organization faces when they are hit by a threat event 'TE41 - Ransomware attack'. The reason the ransomware attack would be successful is because of vulnerabilities across different layers, and these are identified as V41, V42 and V43 in Figure 35.

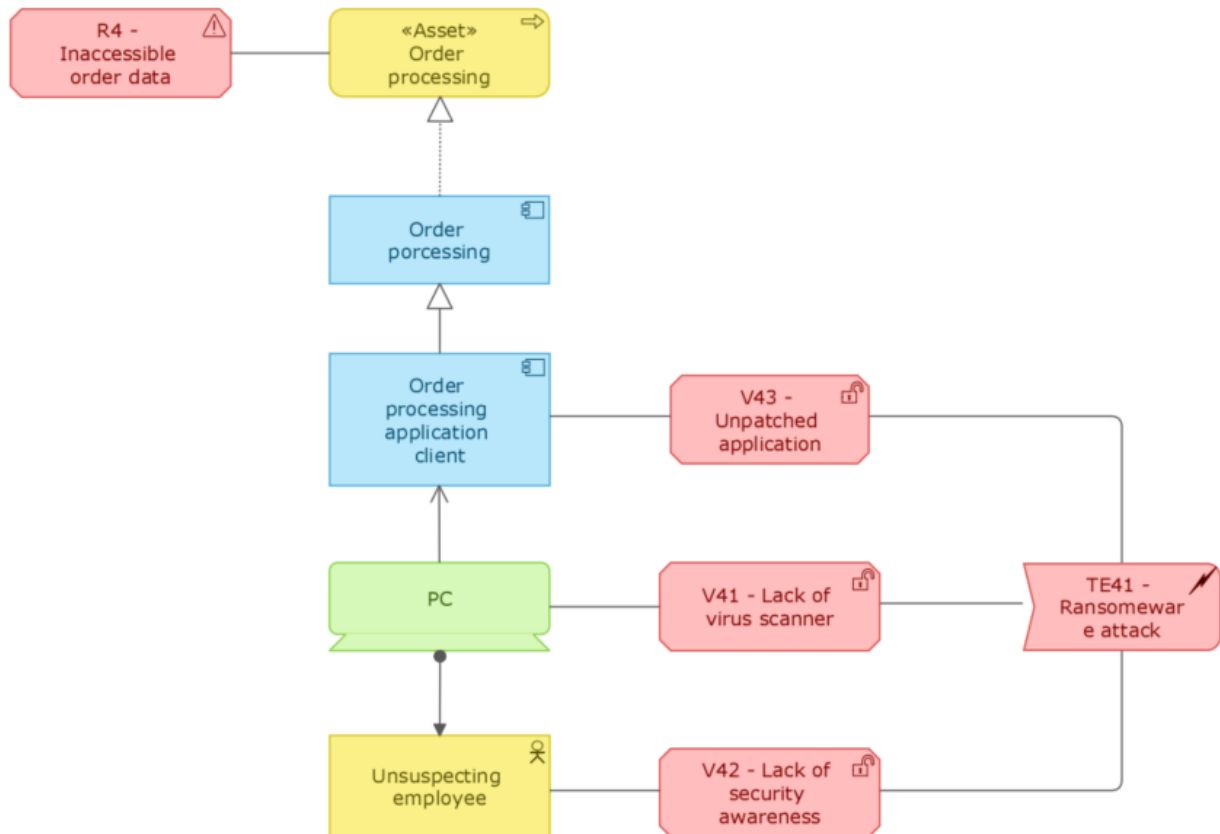


Figure 35 Vulnerabilities and threat identification for attack scenario 2

- Populate metrics

For the next task, we would be filling metrics in the attack scenario. These metrics are determined from the risk and security concepts.

The following metrics are populated:

R4 - Inaccessible order data

Primary Loss – 10000 EUR

Secondary loss – 0 EUR

Uncertainty – Medium (15%)

TE41 - Ransomware attack

Threat events per year – 2.000

As none of the vulnerabilities are CVEs, we do not have to populate any metrics for them.

- Create attack defence graphs

The next task is to create attack graphs following the modelling convention defined in the previous chapter. A new risk and security view is created for this and elements identified earlier in this stage are modelled as an attack graph. The end result of the graph is shown in Figure 36.

The risk scenario is created on the basis that the attacker can either use social engineering attack to infiltrate the corporate network and deploy ransomware, or they could use an unpatched application to enter the network. The OR junction indicate that either of these paths can be successful in reaching the root node. Further, for being successful in the social engineering attack, they would have to exploit two vulnerabilities V41 and V42. Both these have to be true; the employee is unaware how to spot a phishing email, and the IT infrastructure is unable to detect the email delivering the malware exploit.

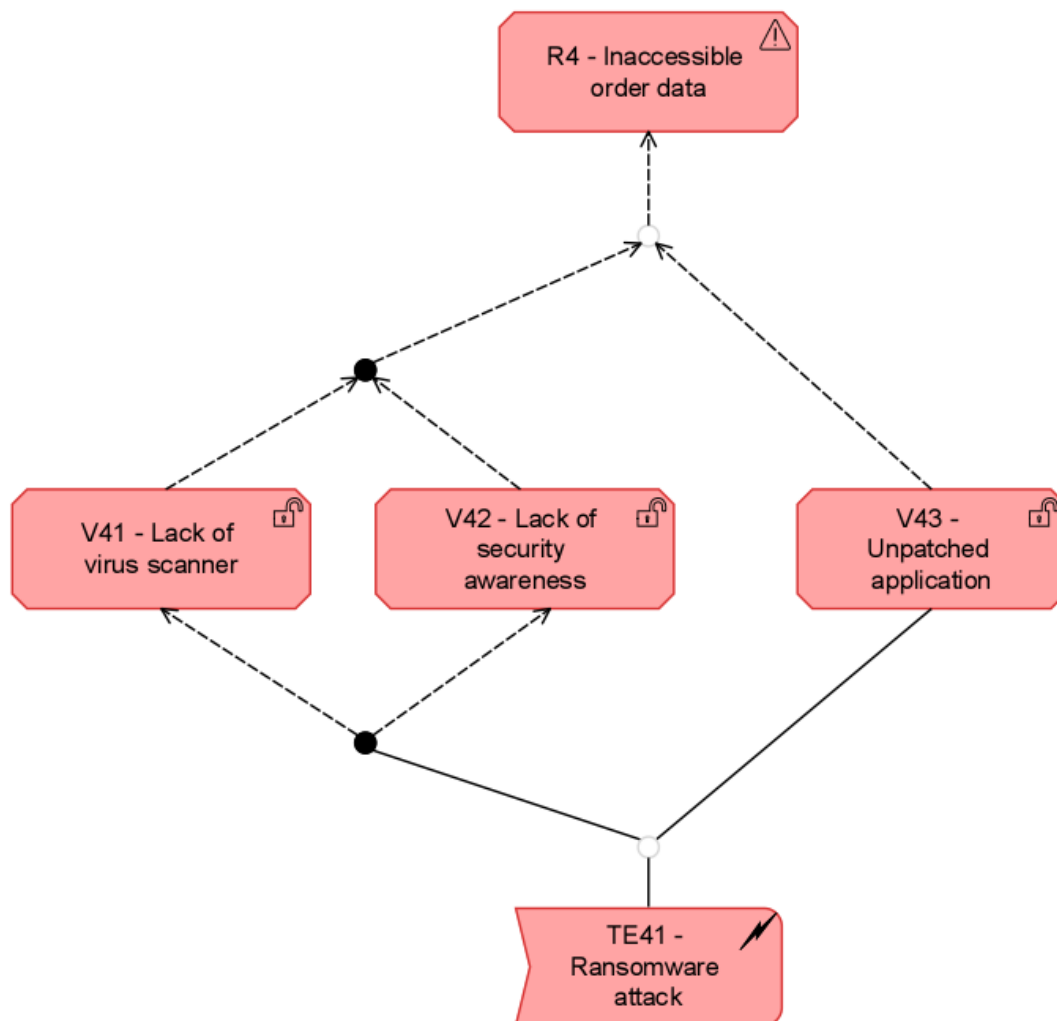


Figure 36 Attack graph for attack scenario 2

- **Fill compute probabilities of success**

The next task is to define probabilities of success in the attack graph. For there are two ways, one is based on the exploitability score for vulnerabilities, given in equation (5.1), and the other is an estimation based on Table 14. As in the current attack scenario, there are no CVE vulnerabilities, we cannot derive the probabilities using the formula and hence make an estimation.

In Figure 37, the probabilities of success have been added to the attack graph. The blue comment boxes are the ones that are manual inputs based on the analyst's assessment of how likely is that particular attack path. The comments in yellow are probabilities that are derived for the vulnerability and risk elements. These are based on the formulae proposed in the design chapter.

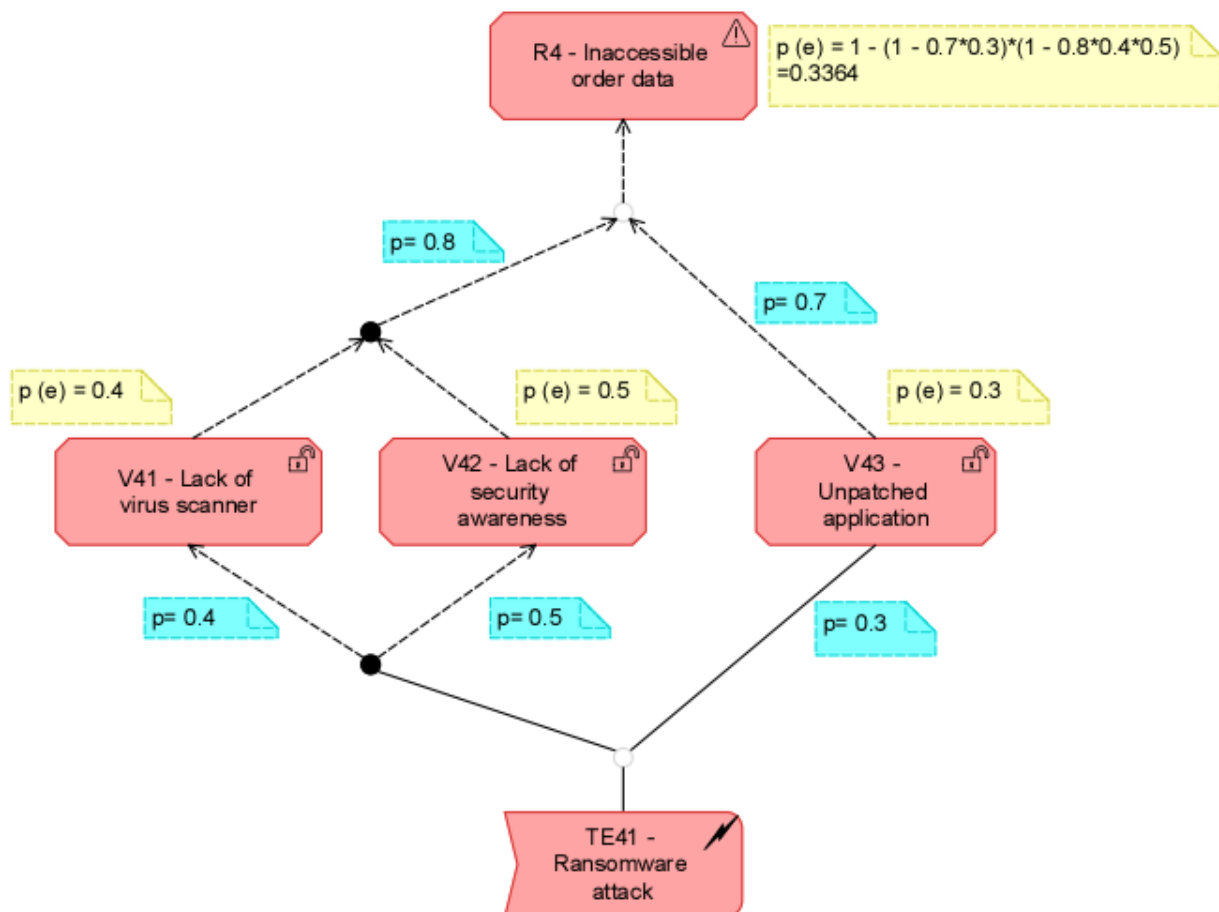


Figure 37 Attack graph with probabilities of success filled and computed

6.3. Stage 3 – Risk analysis

- Compute inherent risk

The next task is to compute Loss event frequencies, Loss Magnitude, and inherent risk in the attack scenario. As per designed approach, the loss magnitude and risk metrics are associated with risk element and the LEF is associated with vulnerability and risk elements in the graph. These calculations are updated in the model and shown as comments in Figure 38.

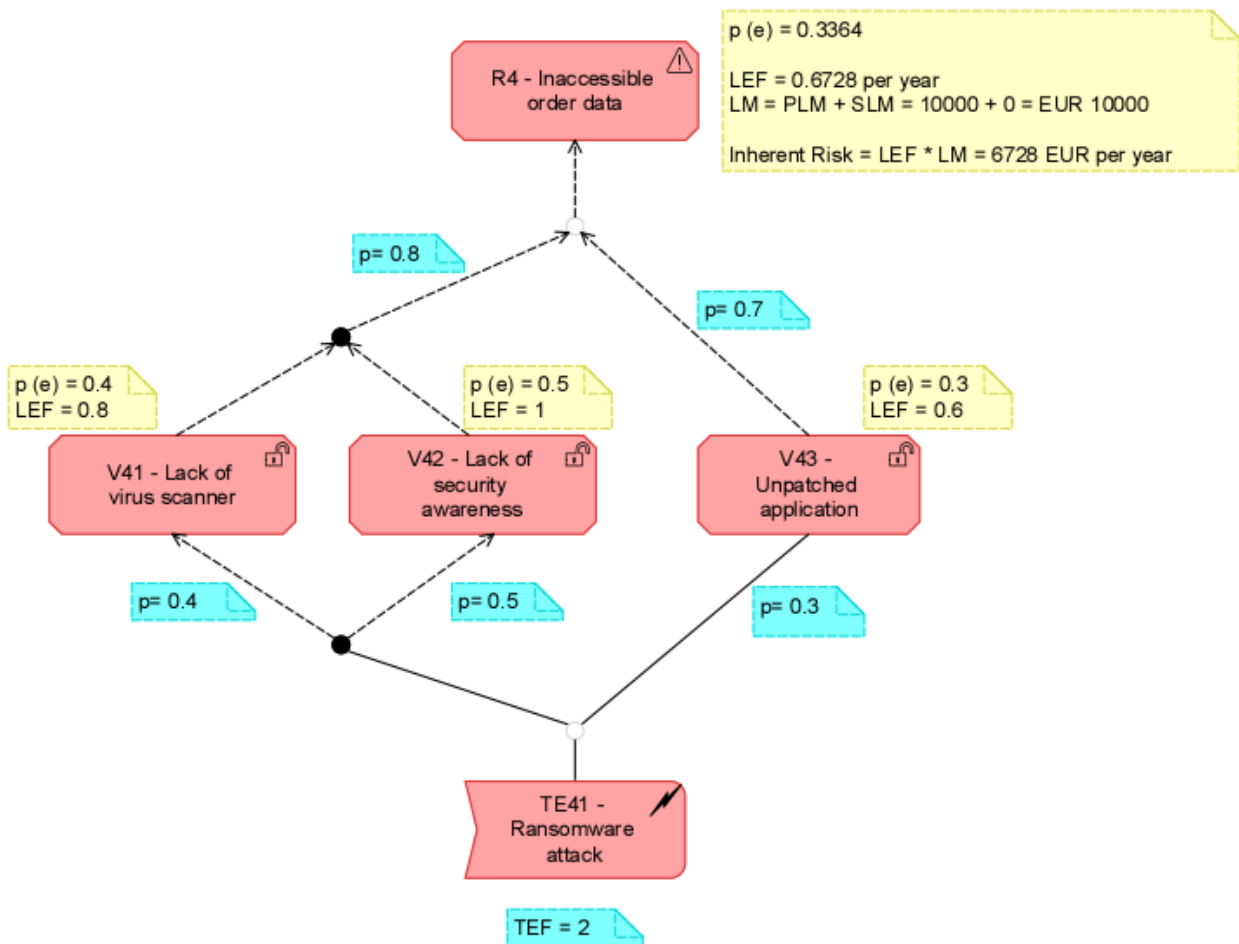


Figure 38 Attack graph with inherent risk calculations added

6.4. Stage 4 – Risk evaluation

- Evaluate risk with risk appetite and risk tolerance

The next task is to evaluate the risk with organizational wide parameters of risk tolerance and risk appetite. As mentioned in stage 2, in this attack scenario we are not defining process risk tolerance, so the organization risk tolerance is used in the computation logic. Using the script for generating colours based on the proposed algorithm, Figure 39 is produced.

Calculations:

ORT = 10%

PRT = Not defined

Organization Risk appetite = EUR 10.000

Asset Value = EUR 1.000.000

Residual Risk (process) = 6728 EUR per year

Using the proposed algorithm,

Process risk tolerance = 10000

Org Risk < Org RA

The process would be coloured **green**

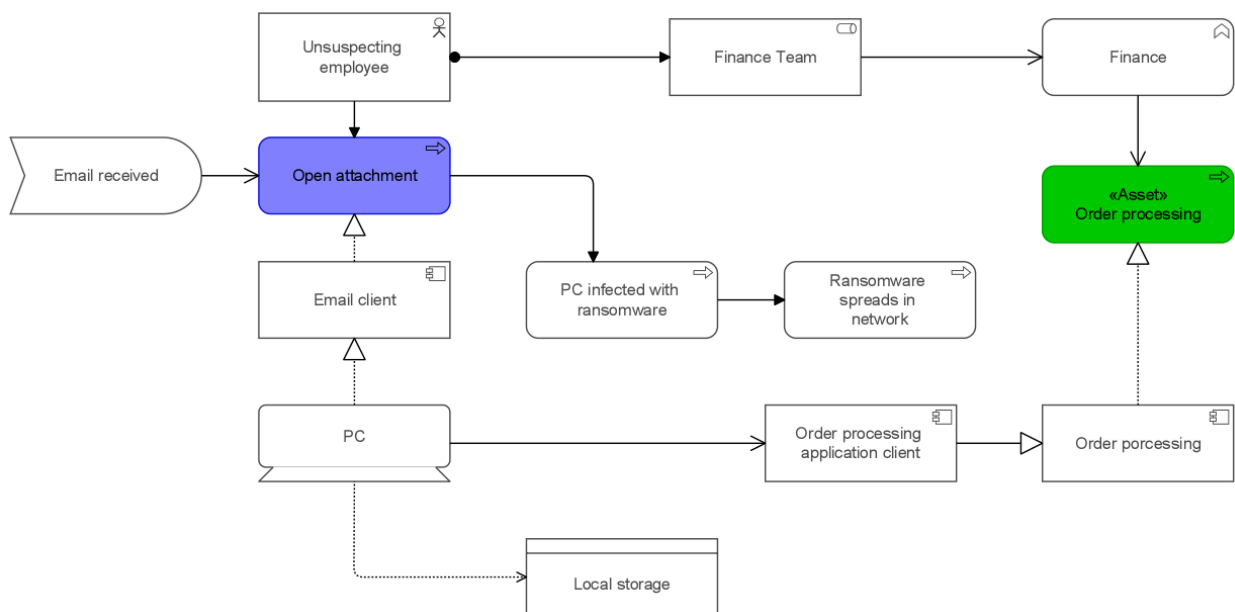


Figure 39 Risk evaluation through colour view for attack scenario 2

6.5. Stage 5 – Risk treatment

- Select and apply controls

The next task for the security analyst is to select and apply controls that can minimize the risk. In this stage, the controls are selected from the ones the SOC is capable of offering. Figure 41 shows the available controls that ArchiMobile has with them. From these controls, the analyst selects the controls which can lower the inherent risk in the attack scenario. These are then added to the attack graph to produce an attack defence graph, as shown in Figure 40.

The controls selected in this scenario are RA-05, which is attached to V41 and V43, and IR-08 attached R4.

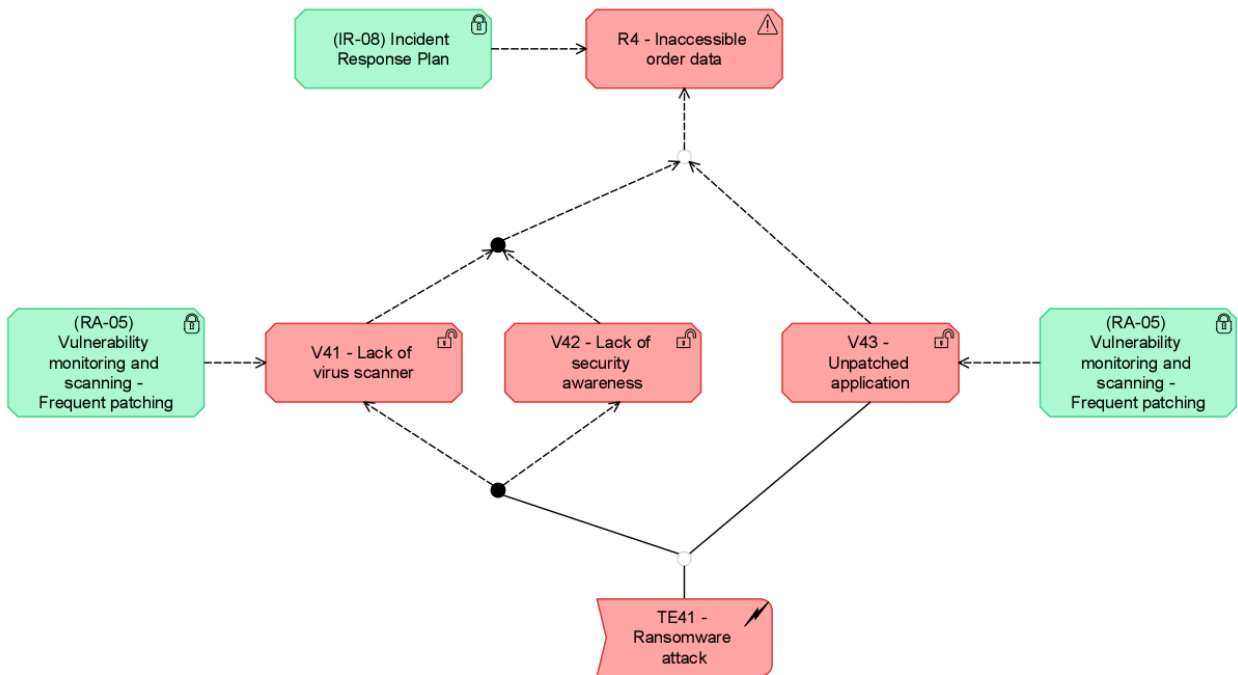


Figure 40 Attack defence graph for attack scenario 2

Controls portfolio Scorecard	Control measure cost	Control measure strength	Control type
(SC-05) Denial of Service Protection	€ 700.00	7	Avoidance
(RA-05) Vulnerability monitoring and scanning - Frequent patching	€ 200.00	6	Vulnerability
(SC-09) Transmission Confidentiality	€ 400.00	6	Avoidance
(AC-02) Account Management	€ 100.00	8	Deterrent
(AC-06) Least Privilege	€ 600.00	8	Deterrent
(SC-10) Network Disconnect	€ 400.00	5	Responsive - LM
(AC-03) Access Enforcement	€ 600.00	7	Avoidance
(AC-07) Unsuccessful Login Attempts	€ 300.00	4	Avoidance
(SC-08) Transmission Integrity	€ 300.00	4	Avoidance
(IR-04) Incident Handling	€ 700.00	7	Responsive - LM
(SI-05) Security Alerts, Advisories, and Directives	€ 1000.00	7	Avoidance
(IR-08) Incident Response Plan	€ 500.00	6	Responsive - LM
(IR-07) Incident Response Assistance	€ 900.00	8	Responsive - LM
(SI-04) Information System Monitoring	€ 300.00	3	Avoidance
(IR-06) Incident Reporting	€ 800.00	6	Responsive - LM

Figure 41 Portfolio scorecard of controls

- Compute residual risk

The next task is to compute the residual risk and the associated LM and LEF values in the attack defence graph. The computation is shown in Figure 42, and residual values are mentioned with the prefix 'res'. As the residual risk values are satisfactory here, we move on to the next task. The control strength of the controls affects how much of the risk is reduced. The residual LEF is calculated for V41, V43 and R4, while LM and Residual risk is calculated for R4. These are done using the equations (5.12) and (5.14).

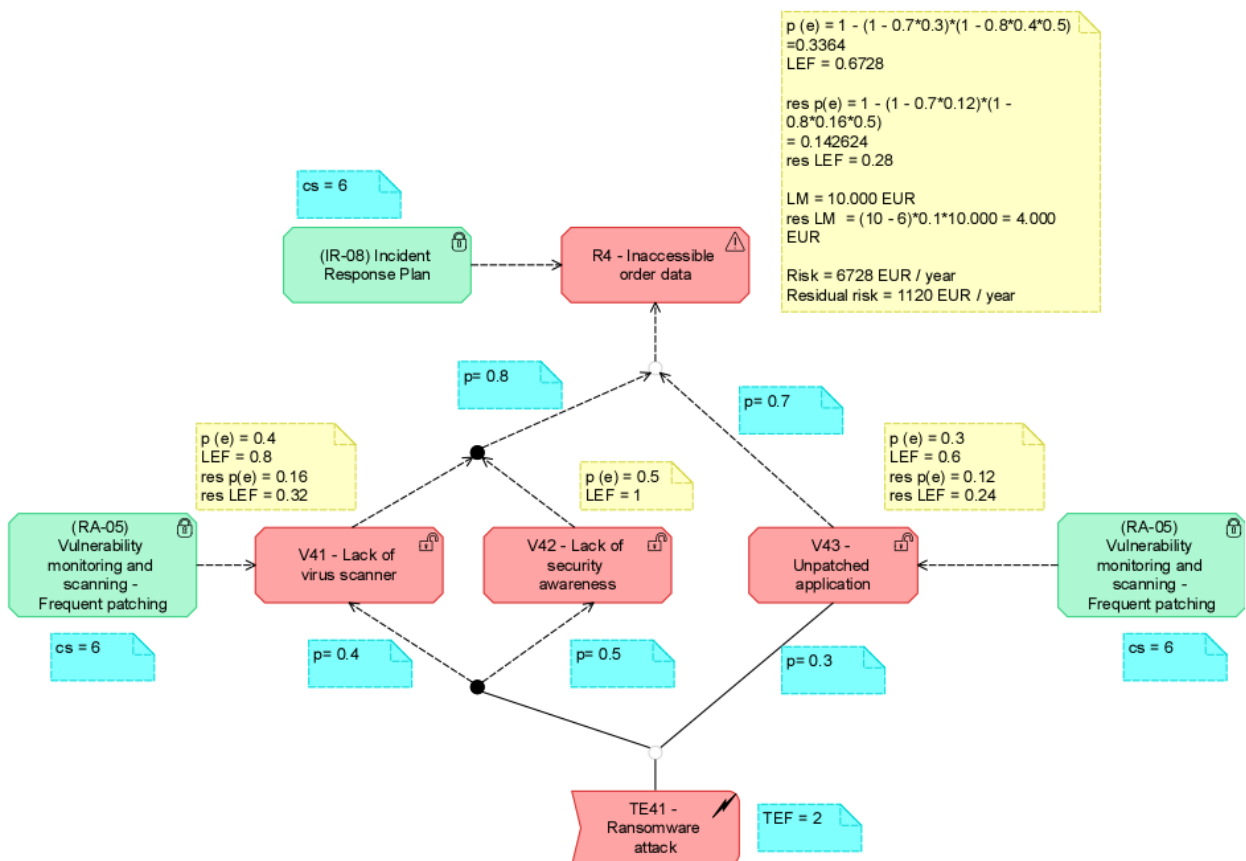


Figure 42 Residual risk calculations for attack scenario 2

- Compute return on security investment

Next, the return on security investment is calculated by using the provided formula. The ROSI is displayed on the same view as the attack graph and uses the scorecard chart option in BiZZdesign Enterprise Studio. Figure 43 shows how the value is displayed, including the calculations of how it is arrived at. An analyst would be able to identify when applying controls, the value of ROSI in the attack scenario and choose the most optimal set of controls based on the objective to minimize the ROSI value. In our scenario, we are satisfied with the selection and choose to move forward to the next task.

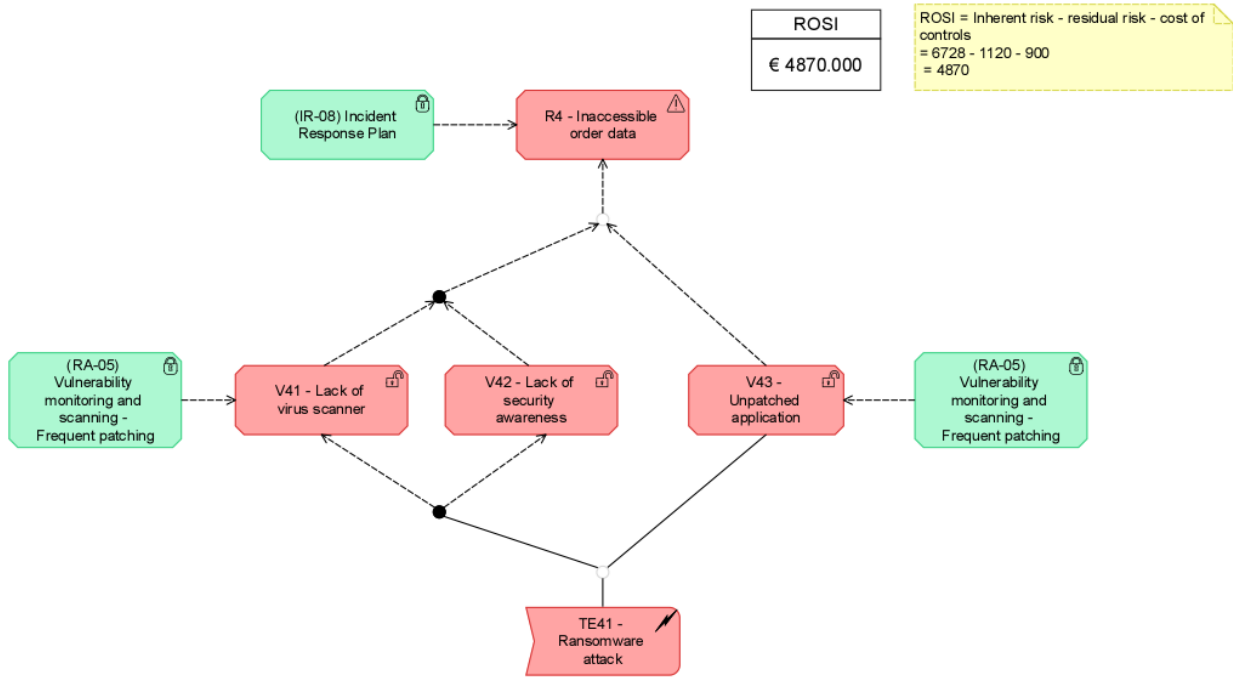


Figure 43 Return on Security calculations on attack scenario 2

Compute risk exposure

The next task is to compute the risk exposure. This would show how the organizations total risk exposure increases with modelling this attack scenario. In line with the previously defined constraint, the risk is mutually exclusive with other risks in the organization, thus can be added with the existing exposure.

The analyst would then need to manually execute a script that would update the value of risk exposure in the organization’s stakeholder concept. The updated risk exposure is shown in Figure 44.

Metrics		Basic profile	
Metric		Value	
Organizational risk appetite		10000.000	
Organizational risk tolerance (%)		10.000	
Total Risk exposure		7148.000	

Archimobile

Figure 44 Updated risk exposure for ArchiMobile

6.6. Stage 6 – Monitor risk

- Inform decision-makers

The next task in our approach is to inform decision-makers. This step can vary depending on how the organization chooses to communicate the findings. These can be through reports, emails or dashboards. As ArchiMobile is heavily using Enterprise Studio, we have created a dashboard that communicates the risks identified and the various metrics related to it. This dashboard can be viewed by different stakeholders who are using Enterprise Studio and can be customized according to their needs. In Figure 45, we present a dashboard created for the attack scenario. It includes organizational metrics, risks, vulnerabilities and business processes in line with the principles for communicating risk defined in the design of our approach.



Figure 45 Dashboard for communicating with decision makers at ArchiMobile

- Monitoring risk

The next task is the monitoring of risk, which is a continuous activity. Here we may update any new vulnerabilities, threats or assets identified for the risk scenario. These are then updated in the attack defence graph, and the complete process can be applied again.

In our scenario, we assume that during the monitoring stage, the organization is growing well, and the value of asset increases. The stakeholders thus decide to change the process risk tolerance and set it to a lower value because they are more risk-averse now.

Old value of asset = 1.000.000 EUR

New value of asset = 2.000.000 EUR

Old process risk tolerance = <<unset>>

Process risk tolerance = 4%

After setting these values in the model, the analyst has to go through the risk evaluation again. The result of the generated colour view is presented in Figure 46. While in this case, new vulnerabilities and risks were not added to the attack scenario, it might be the case that after a period of time, the attack surface changes or new vulnerabilities are discovered, which would have to be updated in the attack graphs.

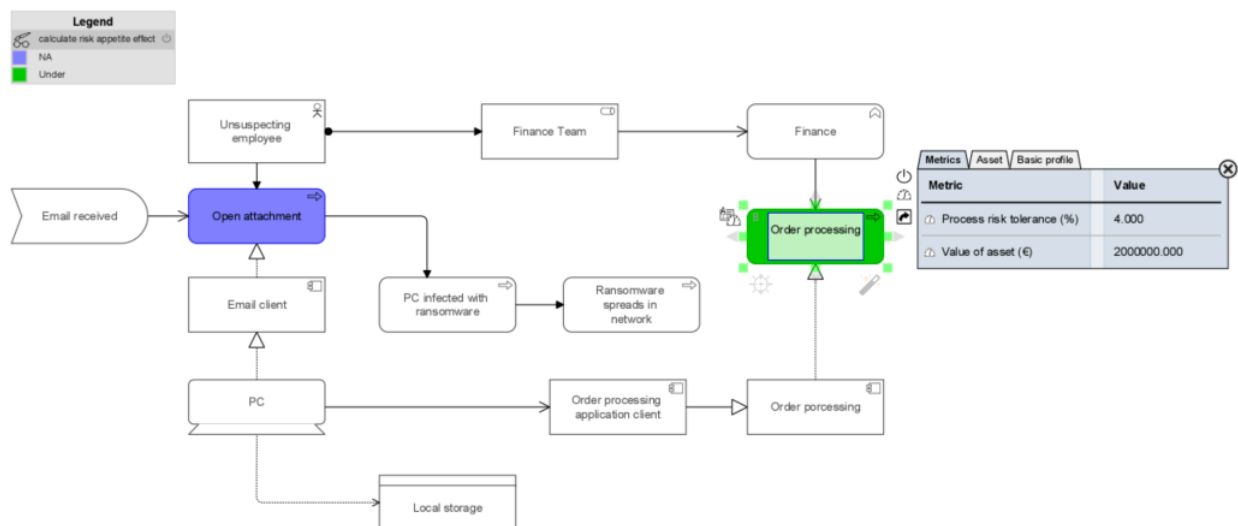


Figure 46 Monitoring risk for attack scenario 2

6.7. Requirements satisfied

In this section of the validation chapter, we would be going through the requirements that were initially identified during research design to test if they are satisfied. Each of the requirements is analysed by the author to see if they are satisfied and marked as Yes, No or Partial.

Table 25 shows the functional requirements evaluated against the proposed design. FR1, FR2, FR3, FR5, and FR7 are completely satisfied, while FR4, FR6, and FR8 are partially satisfied.

- **FR1** – this is completely satisfied as the MORSE approach is quantitative in nature. The inputs, calculations and outputs are all estimated in numeric terms. This is an improvement over the existing qualitative assessment that was earlier performed.

- **FR2** – This is completely satisfied as we are using ArchiMate modelling language for developing the models of the enterprise as the basis. Moreover, risk scenarios are modelled as attack graphs which are also structured representations.
- **FR3** – this requirement is completely satisfied as the resultant risk is in currency terms, and the risk analysis involves estimating the expected loss to the business. As the FAIR methodology is used, which defines the different forms of losses (Figure 17), it captures the various impact the business might face from cyber threats.
- **FR4** – This requirement is marked as partially satisfied. This is because while our approach provides a way to select control measures using a portfolio-based approach, a risk analyst may already be aware of available controls in SOC. There is no mechanism to see a subset of controls that would be applicable in the scenario. This leaves scope for improving the design to completely satisfy this requirement.
- **FR5** – This requirement is satisfied and is similar to **FR2**. MORSE uses ArchiMate, which is an EA modelling language. Further, it links the different layers of EA together where cyber risk could be.
- **FR6** – This requirement is partially satisfied. In MORSE, the risk is attached to one element, which is identified as an asset in the risk scenario. There are other elements in the model that are related to the asset but do not receive an individual risk score. This is partially solved by vulnerabilities that are attached to elements, which have the metric for LEF, but that only gives a part of the risk in the model.
- **FR7** – This is completely satisfied. We propose the use of Return on Security Investment to evaluate how beneficial it would be to apply a set of controls to mitigate a risk scenario. The analyst could further see control cost and strength in a portfolio view to decide which controls to apply.
- **FR8** – This is partially satisfied. The approach can be integrated into a SOC, given that they are using Enterprise Studio in their organization and the users are well versed with modelling. Integrating it to an actual SOC is yet to be realized.

Table 25 Functional requirements validation

Sr no.	Functional Requirement	Satisfied?
FR1	The approach provides a quantified risk assessment	Yes
FR2	The approach is model-based	Yes
FR3	The user can perform business impact analysis through it	Yes
FR4	The approach supports a way for selecting appropriate control measures	Partial
FR5	The approach is based on Enterprise Architecture	Yes
FR6	The user can see the propagation of risk through different architecture layers	Partial
FR7	The user can do a cost-benefit analysis of controls	Yes
FR8	The approach can be integrated within a Security Operations Centre	Partial

Next the Non-functional requirements are analysed. These are summarized in Table 26 and explained below. NFR1, NFR2, NFR3, NFR5, and NFR6 are completely and NFR4 is partially satisfied.

- **NFR1** – This NFR is completely satisfied. The approach uses existing standards like ISO31000, Open FAIR, ERSM concepts in ArchiMate and builds on them.
- **NFR2** – This is completely satisfied as we are extensively using features in Enterprise Studio to realize the design.
- **NFR3** – This is also marked as completely satisfied as there are a total of inputs given by an analyst. The number increases as the scenario complexity increases, but we would still consider the number of inputs to be manageable considering the quantitative nature of risk assessment
- **NFR4** – This requirement is partially satisfied. This is because the approach we propose in this research uses parts of the ERSM approach but deviates in terms of creating attack graph-based risk scenarios. Additionally, we do not use all the concepts defined in ERSM in order to manage complexity.
- **NFR5** – This NFR is completely satisfied as one of the steps in the approach is to work out the risk scenario which also helps in identifying the related concepts. The risk is not calculated independent to a particular concept but is rather at a holistic level where the user can identify what all components can be involved in the scenario.
- **NFR6** – This NFR is marked as completely satisfied as this thesis report serves as one part of the documentation. The workshop conducted as part of the research provided a way to assess how the approach can be provided in a training environment. It should however be noted that no separate Training material is prepared which can be readily distributed as part of this assignment.

Table 26 Non-Functional requirements validation

Sr no.	Non-functional Requirement	Satisfied?
NFR1	The design can be built reusing existing methods	Yes
NFR2	It should be demonstrated in BiZZdesign Enterprise Studio	Yes
NFR3	There should be limited number of inputs	Yes
NFR4	It can extend the existing ESRM approach in ArchiMate	Partial
NFR5	There can be a scenario-based approach to model risk	Yes
NFR6	There should be documentation / Training to educate analysts on the proposed approach	Yes

In the next chapter, we would perform an evaluation with an external panel of experts.

7. Evaluation

The next and final phase in the design cycle for DSRM is implementation evaluation. In our research, we use this chapter to describe how our proposed approach would work if it is deployed in a real-world implementation. The evaluation of this thesis research is performed using the validation method of expert opinion method mentioned by Wieringa (2014) [6]. Additionally, while planning for evaluations, the thesis of Vaicekauskaitė (2020) [70] was referred.

7.1. Evaluation structure

The artefact is evaluated through employees of BiZZdesign in different roles. For them, the application in the real-world would be that the approach is used by customers of BiZZdesign. While it was not asked explicitly in the questionnaire, it is assumed that the participants spent a considerable amount of time with customers and are aware of the real-world problems that they are trying to solve. Also, considering that there is an increased awareness about cybersecurity in organizations, it is good practice to consider security aspects when dealing with any kind of work.

A mini-workshop was organized online on 15-July-2021, in which five employees with different roles were invited. The workshop was for 2 hours and was divided into three segments. The first 45 mins were for introducing them to MORSE through a PowerPoint presentation. The next 45 mins were for demonstration, hands-on exercise, and discussion. And the last segment for 20 mins was reserved for filling a questionnaire that had eight questions, as described in the following sections.

During the workshop, the presentation lasted for about 50 mins. After the introduction, it was checked how the participants would like to proceed, and it was agreed to first have a demonstration of the approach and then a discussion. The questionnaire was shared after the initial presentation so that the participants would know what criteria they would evaluate it against. The artefact was demonstrated by screen sharing Enterprise Studio and walking through each of the steps of the process. Attack Scenario 1, which is described in the Design chapter, was demonstrated which took about 45 mins in the workshop. After the demonstration, the participants were asked if they would like to try out using the model. However, it was agreed by everyone that a discussion following the demonstration would be fruitful. The final 30 mins of the workshop were for discussing the proposed design and answering questions. These have been described later in this chapter.

7.2. Participant profile

As part of organizing the workshop, a focus group of 5 experts were invited to the meeting to give their opinion on the artefact. One commonality was that they were all employees of BiZZdesign, the organization supporting this research. A summary of the participants' profiles is given in Table 27. All the experts in the focus group had at least 12

years of experience with EA. The experience with security & risk varied from 0 to 10 years. It should be mentioned that two of the participants in the workshop were involved since the start of the research, while the other three were introduced to the artefact during the workshop. Additionally, as BiZZdesign is a research-driven organization, thus several of the participants also had considerable experience with academic research and methodology. This was considered important in the context of Master thesis research.

However, one limitation identified in the participants profile is that none of them would be the end users of the proposed approach, as the target audience is risk managers and security analysts working in SOC. We consider that given the extensive experience of our participants, who work with different organizations as part of their day-to-day work, they would make experience-based judgment of how the artefact may be used by end users.

Table 27 Participant's profile

Participant id	Organizational role	Experience with EA (years)	Experience with Risk/Security (years)
A	Consultant	20	2
B	Consultant	15	10
C	Global Director of Presales	13	5
D	Research engineer	15	0
E	Chief Strategy Officer	12	4

7.3. Questionnaire

To gather inputs from the participants during the workshop, a questionnaire was prepared comprising of eight questions. We used the UTAUT (Unified Theory of Acceptance and Use of Technology) method [71] for formulating the questions. We choose this method because we want to test how the MORSE approach would be accepted in practice. As our approach is a novel creation, the target users may be hesitant in the beginning to adopt it. The UTAUT method analysis how widely a new technology may be accepted with the users based on 4 four determinants of behavioural intention and usage behaviour - performance expectancy, effort expectancy, social influence, and facilitating conditions, and up to four moderators of key relationships. The questions in this questionnaire are based on these aspects of the UTAUT method.

The eight questions that are formulated are shown in Table 28. These are also formed on whether the Functional and Non-functional requirements initially specified are fulfilled and if the proposed approach would be useful in their opinion. The approach was still unnamed at the time of the workshop, and the questions were formed with the word 'proposed approach' referring to MORSE. The use of each of the construct is explained in the next section of this chapter along with why each of the questions was formulated.

Table 28 Evaluation questionnaire

Question Nr.	Root construct	Property	Statement
Q1	EE- Effort expectancy	Perceived ease of use	The proposed approach is easy to use in practice.
Q2	FC - Facilitating conditions	Compatibility	The proposed approach is compatible with existing customer use cases for risk and security.
Q3	PE - Performance expectancy	Perceived Usefulness	The proposed approach adequately captures business impact for a risk.
Q4	FC- Facilitating conditions	Perceived Behavioural Control	I would be able to find adequate knowledge and support about applying the approach in practice.
Q5	PE - Performance expectancy	Perceived Usefulness	The approach captures the propagation of cyber risk effectively in Enterprise Architecture models.
Q6	PE - Performance expectancy	Relative Advantage	The proposed approach would allow for better selection of control measures to mitigate risks.
Q7	PE- Performance expectancy	Perceived Usefulness	Applying the proposed risk quantification approach improves the ability to communicate about risk within an organization.
Q8	PE- Performance expectancy	Job-fit	Using the proposed approach at a Security operations centre would lead to improved decision-making when responding to threats.

- Construct definitions

The definition of the constructs and properties as provided by Venkatesh et al. [71] are given below. The first three are root constructs (RC) and the rest are properties.

- **Effort expectancy** – It is defined as the degree of ease associated with the use of the system.
- **Facilitating conditions** – they are defined as the degree to which an individual believes that an organizational and technical infrastructure exists to support the use of the system.

- **Performance expectancy** – It is defined as the degree to which an individual believes that using the system would help him/her attain gains in their job performance. enhance their job performance
- **Relative Advantage** – the degree to which using an innovation is perceived as being better than using its precursor
- **Perceived Usefulness** – The degree to which a person believes that using a system would
- **Job-fit** – How the capabilities of the system enhances an individual’s job performance
- **Perceived ease of use** – the degree to which a person believes that using a system would be free of effort
- **Compatibility** – The degree to which an innovation is perceived as being consistent with existing values, needs and experiences of potential adopters.
- **Perceived Behavioural Control** – reflects perception of internal and external constrains on behaviour and encompasses self-efficacy, resource facilitating conditions and technology facilitating conditions

- Scale

A Likert-type scale was defined to collect responses from the participants. The scale ranged from 1-5, and the values were mentioned as: 1 – Strongly disagree, 2 – disagree, 3 – neither agree nor disagree, 4 – agree, 5 – strongly agree. The results table highlight the different values by colours ranging from dark red to dark green correspondingly.

For each question, the participants could also give their positive and negative opinions to expand about their (dis-)agreement to the statement. All the questions were kept as optional for the participants, but it was mentioned to them that there are a limited number of responses that are collected for the research. The questions were marked optional because not everyone may have an opinion on each of the statements.

7.4. Results

The questionnaire was distributed through an online form link during the workshop. The participants were given time to answer the questions during the workshop and later through the day. The responses were then exported as a CSV file and processed in a spreadsheet. All responses to the questionnaire are provided in Appendix 2 of this report.

Table 29 summarizes the responses we received. We also compute the median and standard deviation for each of the questions. The median value is calculated for the answers to measure the most frequent choice. Elaine & Seaman (2007) [72] mentions that mean and standard deviation values are invalid with a Likert scale because of the ordinal scale and thus suggest median for analysis. However, we still calculate the standard deviation but have no intention to use the value. With standard deviation, we measure the dispersion of values in the set of data values. A high standard variation indicates that there is a wider gap of ratings from the participants. The responses to the questionnaire are provided in Appendix 2 of this report.

RC	Questions	Participants					Median	Standard Deviation
		A	B	C	D	E		
EE	Q1: The proposed approach is easy to use in practice.	3	3	4	2	2	3	0.837
FC	Q2: The proposed approach is compatible with existing customer use cases for risk and security.	3	4	4	N A	4	4	0.500
PE	Q3: The proposed approach adequately captures business impact for a risk.	3	4	4	4	4	4	0.447
FC	Q4: I would be able to find adequate knowledge and support about applying the approach in practice.	3	3	3	4	3	3	0.447
PE	Q5: The approach captures the propagation of cyber risk effectively in Enterprise Architecture models.	4	4	4	4	5	4	0.447
PE	Q6: The proposed approach would allow for better selection of control measures to mitigate risks.	3	4	3	4	4	4	0.548
PE	Q7: Applying the proposed risk quantification approach improves the ability to communicate about risk within an organization.	4	4	3	3	4	4	0.548
PE	Q8: Using the proposed approach at a Security operations centre would lead to improved decision-making when responding to threats.	3	4	4	4	4	4	0.447

Table 29 Summary of evaluation questionnaire responses

Q1: The proposed approach is easy to use in practice.

For a process to be widely adopted, it is important that it is easy to be applied. Through this question, we attempt to gauge how the experts feel about the proposed approach. If the approach is easy to use in practice, then it means that the user can spend more time performing their job than learning how to use it. The question measures the 'effort expectancy' construct from the UTAUT model. Perceived ease of use for the participants is based on the demonstration they received of the artefact. We measure how the participants feel MORSE would be easy to use for their customer by responses to this question. Due to the limited time of the workshop, none of the participants went for the 'hands on' exercise, so it was based on observation instead of actual use.

Response: Median – 3; Standard deviation – 0.837; Min – 2; Max – 4

The median score for this question is 3, which indicates that the approach is not very easy to use in practice. The standard deviation is the highest amongst all the questions, which means that there is a divided opinion on this. One known limitation in our approach, which is also related to this question is that experts in our evaluation are not the target user base for the approach. Participants D & E rated this question as 2 and C rated it highest at 4.

The participants gave positive feedback that the approach is well structured with a clear description of steps and activities. Additionally, for people who are experienced with modelling it would not be difficult. The negative feedback was also regarding the modelling experience as the general community expected to use the approach – risk managers would not have the modelling experience. Additionally, it was mentioned that there would be a substantial amount of work required to carry out the assessment. However, it was also by one participant that there may not be any easy way to do it in practice.

Q2: The proposed approach is compatible with existing customer use cases for risk and security.

This question is formulated to check how compatible is the proposed approach with existing ways of performing a risk assessment. We are measuring the ‘compatibility’ property in UTAUT. As the approach is based on the qualitative implementation of Open FAIR in ArchiMate, we want to know if it can be easily upgraded. As Enterprise Studio already has the functionality to do the qualitative risk assessment, customers who are using them can also start using the quantitative method. While an actual comparison would be difficult to estimate at this stage, the existing example of ArchiSurance in ES can give a way to compare. It was posed to the participants because they are in customer-facing roles and would have a fair understanding of their values, needs and experiences of potential adopters.

Response: Median – 4; Standard deviation – 0.500; Min – 3; Max – 4

3 out of 4 participants rated this question as a 4, which indicates that they largely agree with it. One of the experts did not rate this question, as their experience with risk/security was zero years. The ratings indicate that the experts believe that the approach can be implemented in real-world cases, and users of the qualitative approach can possibly be upgraded to use MORSE.

From positive opinions, they indicate that the approach fits well as an extension to architecture activities. Another positive was that risk and security are not considered while modelling EA, and if this approach is used, then it can be done as an in-parallel activity. Negative opinions seem to be of two forms – one that risk is a very board topic, and the other being same as previous answer, that security teams would not be using modelling tools. This would imply that there would be few practitioners who would be skilled at security modelling.

Q3: The proposed approach adequately captures business impact for a risk.

One of the initial requirements was that the design of this risk assessment approach should be able to capture business impact for security incidents. As Enterprise Architecture models are a way to communicate to business users, we would want the approach to be

meaningful for decision-makers who may in in the role of Business Unit head, Executives, and CxOs. We are measuring the ‘perceived usefulness’ property of MORSE which would tell us how using it would enhance their job performance.

Response: Median – 4; Standard deviation – 0.447; Min – 3; Max – 4

The experts largely agree with this statement, with 4 out of 5 rating it 4. This indicates that they see the business impact being captured through the calculations of risk in the approach.

Positive opinions on this statement indicate that expressing money value is a good starting point, as is capturing business metrics, which, while not explicitly mentioned, we would assume to be Loss Magnitude. LM being a FAIR metric, captures business value well because of the six different forms of losses that the LM can be, and while performing a risk assessment, it is expected those are considered to arrive at a final risk value.

Negative opinions include that the approach does not make it explicit how the business impact is arrived at and there should be deeper explanation around it. Additionally, one of the experts mentioned, which was also discussed during the workshop, that the risks should be summed up for risk exposure, as they may be correlated. This was improved in the theory of the approach, to make it explicit that the risks should be mutually exclusive in the risk assessment process. Another participant pointed out the uncertainty in the value should be made (more) explicit.

Q4: I would be able to find adequate knowledge and support about applying the approach in practice.

The users for the approach should be able to gain sufficient knowledge to correctly perform risk assessment. If there are discrepancies in their knowledge, they should be able to clarify it by referring to available documents. Through this question, we aim to analyse how what the participants think about their ability to find more information in case they are stuck at a task of the approach. The participants were made aware that the approach users many industry standards in its development, which are generally freely available to refer through the internet. The UTAUT property ‘Perceived Behavioural Control’ is measured through this question as we want to measure the experts’ perception about having sufficient resources to work with MORESE.

Response: Median – 3; Standard deviation – 0.447; Min – 3; Max – 4

The response to this question is in the middle. 4 out of 5 participants rated it 3, which means neither agree with it nor disagree. This would imply that there is a scope to improve the delivery of knowledge to correctly apply this approach in practice. This can possibly be covered through a dedicated training manual which could be used by analyst till they become proficient in using the approach.

Positive opinion on this statement indicate that MORSE was presented well, along with examples as illustration. One expert mentioned that further knowledge can also be found using Open FAIR documents, which are indeed freely distributed by The Open Group.

Negative opinion on this statement include, Open FAIR is not well documented for end-users, the large number of inputs needed may be challenging to find, and there can be an end-to-end explanation. The last part was addressed through the Demonstration chapter in this report.

Q5: The approach captures the propagation of cyber risk effectively in Enterprise Architecture models.

Enterprise Architecture offers to combine different elements of an organization for efficient operations and execution of strategy. As the approach is basis the risk assessment on EA, we want to measure how effective the participants feel that it combines the two. Thus, how the cyber risk is seen as propagating through the different layers of ArchiMate model of the enterprise. This question also measures the 'Perceived usefulness' property of the 'performance expectancy' construct in UTAUT. It was a requirement (FR6) that the proposed approach should be able to capture how the risk would propagate within ArchiMate layers, and we measure how successful this is according to our experts.

Response: Median – 4; Standard deviation – 0.447; Min – 4; Max – 5

There is an agreement here that the approach captures propagation of risk effectively in EA models. With 4 out of 5 experts rating it a 4 and 'participant E' rating it 5, which means they completely agree.

Experts mention that ArchiMate concepts are clearly linked to risk concepts and high-level elements were identified well in the approach.

Negative comments mention – propagation of risk can be more explicit, and lack of link between the layers, i.e., how do the risk elements relate to assets. They requested that this is explained better, and it was subsequently incorporated while creating this report. In the second stage, a new view is created where asset and the corresponding elements are modelled. In this view, we identify vulnerabilities and threats, which are attached to the core ArchiMate concepts. The RSO elements are then used to create the attack graphs in a new view.

Q6 The proposed approach would allow for better selection of control measures to mitigate risks.

As part of the risk assessment process, a key outcome is to act on the result and thus lower the risk. For our proposed approach, we would like to measure what the participants think about using the approach to make more informed decisions to select countermeasures to vulnerabilities. We propose to have a portfolio-based approach in selecting control measures and measuring the return on security investment to optimize the selection of controls. Through this question we assess if this is going to be a better strategy to choose the right control measure. This question measures the 'Relative advantage' property in 'performance expectancy' construct.

Response: Median – 4; Standard deviation – 0.548; Min – 3; Max – 4

This statement led to a mixed but positive response. Three participants rated 4 and two participants rated it a 3. This indicates that the approach only slightly provides a way to better select control measures according to our selected experts.

Positive opinions appreciated the use of a standards-based approach (for control measure catalogue), the use of Return on Security Investment and following a model-based approach. Using existing standards in practice should add good value, as organizations already have adopted them and would be looking to expand coverage to maximize security tools utilization. However, one expert, while agreeing that modelling controls is efficient, warned that it depends on the models/modelling being in place. This we infer as organization should have large parts of their enterprise available in models for our approach to be beneficial.

Negative opinions – lack of details in control measure selection. This part was apparently not clearly covered during the workshop which we believe led to this comment, and we believe that with this report, the approach should be clearer.

Q7: Applying the proposed risk quantification approach improves the ability to communicate about risk within an organization.

An important part of Enterprise Architecture modelling is the ability to communicate to different stakeholders. An improved communication would mean that management and executives understand the risks and possible mitigation actions more clearly at a granular level. And at the same time, Security analyst and risk managers at the SOC can model risks and mitigation actions in a viewpoint. Further the monitoring stage of the process details how the communication to various stakeholders should be for effective risk management. Through this question we assess what the participants feel about the improvement in the ability to communicate across various organizational layers by using this approach. This question measures the ‘perceived usefulness’ property of UTAUT.

Response: Median – 4; Standard deviation – 0.548; Min – 3; Max – 4

The response to this statement is also mixed, with three participants rating it 4 and 3 participants rating it as 3. This indicates that the experts are of the opinion that using this approach would not greatly improve communication of risk within the organization.

Positive opinions indicate that, using this approach would enable decision to be more concrete, lead to better conversation with business stakeholders, value of quantification as it can make technical people get a seat on the executive table, and the approach offers a good foundation for making risk and security explicit.

Negative opinions mention – there may be a need for more visualizations for different stakeholders in the organization and the uncertainty in the numbers should be clarified. We agree to this, that the executives need to have confidence in the results which would only be there if there is clear understanding of the underlying calculations. This can only be achieved when they spend considerable time using the approach, and possibly refining it to suit their needs. Additionally, one expert mentioned that the task of EA would be more about creating architectures (connecting the dots) and consumers of the numbers, and there may be a separate team that works with the number related to risk. We partially agree on this, as risk

management cannot be carried out in isolation, but the approach is intended to be used by risk analyst, who should be well versed with numbers (Loss Event Frequency, Threat Events per year).

Q8: Using the proposed approach at a Security operations centre would lead to improved decision-making when responding to threats.

This question assesses the main objective of this thesis research from the point of view of participants. We would like to measure if they feel that applying this approach would improve decision-making in Security Operation Centres, with the growing threat landscape. The question measures the 'Job-fit' property of 'Performance expectancy' construct in UTAUT and we want to see how well the efficiency of people using our approach would improve. We expect that decision makers could support their decisions by using MORSE, and want to see if the experts also have the same opinion.

Response: Median – 4; Standard deviation – 0.447; Min – 3; Max – 4

A large population of experts agree with this statement, with 4 out of 5 giving a rating of 4. This means that, in their opinion, using this approach would lead to improved decision-making when responding to threats.

Positive opinions mention that the connection between assets all the assets is critical for this and if that can be stressed, decisions can benefit. Another expert mentions that this approach would lead to prioritization of risks and risk treatment.

Negative opinions mention that there may be too much work for SOCs to implement this approach. Some respondents were not familiar enough with workings of SOC to critically analyse this question and they mentioned that through their opinions.

7.5. Discussions during the workshop

During the workshop, the participants were given multiple chances to speak and were eagerly engaged in conversation. The last 30 mins of the workshop were for open discussions. The experts actively participated in the workshop and gave insightful views. The points below are documentation of some of the topics that were discussed.

It was pointed out that the risk exposure should not be a direct sum of all the risk in the organization as the threat events for each of the risks may not be independent. If there are two risk scenarios which have risk that result the same then it must be incorporated into a formula to calculate risk exposure or the assumption should be made clear that the risks are not correlated. An example scenario for this was given as, if an employee is not able to access the office, it could have two cases. One there is a flood in the city and they can't travel to office. Or if the public transport is unavailable, then also the employee cannot reach the office. However, if the city is flooded then the public transport would also not be available. This in this case the two events are related and computing independent risks would not make sense.

The suggestion to include such a situation this was, if there is a correlation between risk scenarios, which should be considered when combining the risk of two events. This correlation can also be part of the calculations for the total risk exposure for the organization. Alternatively, if it is made clear while creating the risk scenarios that the events must be mutually exclusive then this case can be overcome. Thus, in the current form, an analyst would not be able to model such a scenario in which the two events are related in MORSE approach.

Another discussion point was that related elements to the asset are not considered in the risk scenario. That means that if there is a risk to one asset in an organization, e.g., a risk in an authentication service, the dependent elements are not considered in the risk assessment. We do not agree this would be the case if a complete risk scenario is modelled correctly. This was also elucidated out during the discussion. When modelling risk using MORSE, one of the steps is to identify elements which are related to the asset through the model, when looking at vulnerabilities and threats. That means that other elements which have a relation flowing into the asset, and to elements that have relations flowing out are to be considered. This means for an authentication the elements which are utilizing the authentication services are also included in the risk scenario modelling. If there are multiple risks identified, it would lead to different scenarios being created, each with their own set of attack graphs. However, this example is not yet tested, but we expected that it should be possible to model it.

One of the discussions was on the calculations for Return on Security Investment (ROSI). It was mentioned that the formula of ROSI, could be compared with the formula of ROI – Return on Investment, in which there the net benefits are calculated and divided by the cost i.e.

$$ROI = \frac{Benefit - Cost}{Cost}$$

ROI is a performance measure used to evaluate the efficiency of an investment or compare the efficiency of several investments [73]. Using the above formula, the relative gains from making an investment are clear. The author was unaware of this during the discussion, as they had only come across ROSI without the costs in the denominator. However further research into ROSI revealed that there are several researches (including [68, 74]) that use the ROI-type formula for calculating ROSI. However, a study by Onwubiko and Onwubiko (2019) [75] evaluates the formula,

$$RoSI = (Benefits\ of\ Investment - Cost\ of\ Investment) / Cost\ of\ Investment$$

They concluded that it is not clear how to arrive at the ‘benefits of investment’ and further proposed 20 KPIs for measuring security benefits. While this finding infers that the formula for ROSI can include the cost of investment as a denominator for calculations, we chose to keep the formula used in MORSE unchanged as it is also backed by research [61, 62].

Another discussion point was on the sensitivity of calculations. A question was raised if there were analysis done on the sensitivity of change of input values on the resultant values. This analysis was not done as part of this research; however, we did come across the scenario while developing the artefact for validation, that when there is slight change in the input values (Probabilities of success or Number of threat events), there is a significant variance in the calculations. The variance was not measured but observed. In response to that, we had already defined the uncertainty metric. This was also highlighted during the workshop. The uncertainty metric captures such a variance in the values and returns a range for risk. While this is not a complete solution to the sensitivity of the instrument, we believe, it manages to treat a part of the problem. Further research is suggested in this area in the next chapter.

Another related discussion was on the topic of probability distribution of variables and to include a confidence interval in the calculations. It was suggested that the calculations could be enhanced to perform Monte Carlo simulation on the values to return a deterministic computation from the given inputs. This would include a probability distribution for the variables. This was one thing that was thought through during artefact design phase, however we stopped short in the interest of time and complexity considering the research was carried out within a master thesis. However, the Open FAIR Risk Analysis process does suggest that Monte Carlo simulations be applied for risk analysis calculations, and it takes in three inputs for the variables – minimum, maximum, and most likely. This way a triangular probability distribution is created to carry out calculations using repeated sampling of random variables. The advantage of this would be that it would provide a full picture of risk exposure instead of average or most likely [33]. Another approach with FAIR is with Bayesian Networks, and this is described in the Literature Review chapter. It was also mentioned in the workshop that BiZZdesign Enterprise Studio already has such techniques work on probability distributions, and suggested that we look at convolution to implement it. This is added to future work section of this research.

Moreover, including a confidence interval would support decision makers in making informed decisions. When they would see that there is a high confidence in values returned by the system, it would lead to them taking confident decisions. However, we would warn that this should only be in done after thorough testing of the artefact, to not give a false sense of confidence, which might lead to poorer decision-making.

In the next chapter we would provide a conclusion for our research.

8. Conclusion

In this chapter we conclude our research and present our findings with respect to the research objective initially defined. We would be answering each of the research questions based on the artefact designed and evaluated through the research process. Then we would present what are the limitations in this approach, how this research contributes to practice and academics, we would provide opportunities for future research, and finally give our recommendations.

The primary objective of this research was defined as: *Improve decision making at Security Operation Centres (SOCs) through enterprise architecture by designing a model-based risk assessment approach.*

This led to the formulation for the main research question,
How to improve decision-making at Security Operation Centres (SOCs) through an EA model-based risk assessment approach?

To answer this RQ, we formulated seven sub-research question. The answer to these sub-RQ contributes and in turn provides a complete answer to our main research question.

RQ 1: What is the current state of research relating security risk with Enterprise Architecture models, according to scientific publications?

This research question was formulated to create an understanding of prior research and is covered in the Literature Review chapter. For this we conducted a Systematic Literature Review looking at articles published in the past 10 years related to the disciplines of Enterprise Architecture, cybersecurity, and risk. We analysed 29 articles retrieved through the SLR process and classified them based on five concepts covered in this research – Business, Enterprise Architecture, Security, Risk and Analysis, tabulated in Appendix 1. The analysis showed that there are many studies on these topics, but there is a lack of research combining them all. This indicates that there is an increasing interest in these topics, but cross-domain studies are still in their infancy. This is one area that our research has covered by performing a business impact analysis by utilizing Enterprise Architecture modelling techniques. We further extracted metrics, methods and frameworks from these articles which are summarized in the next RQ.

RQ 2: What is the current state of research regarding the quantitative and qualitative assessment of the business impact of security incidents, according to scientific publications?

- **RQ 2a Which frameworks are available to describe the types of impact?**
- **RQ 2b What are the types of costs associated with security incidents?**

For this research question, we went deeper in to the articles retrieved through SLR, and used a data extraction form to capture relevant information from them. To answer all the sub-questions, we collected the metric, frameworks, and methods each of the authors proposed in their research. These are tabulated and described in Section 4.3 of this report.

We found 10 analysis method, 7 frameworks and 7 articles with several metrics in each. All the risk analysis methods that we found were quantitative in nature which indicates that research is focusing on these techniques. This also correlates to exploratory research we conducted that there are more commercial products that offer quantitative risk analysis methods. Further, the frameworks we came across, were classified into 4 topics based on what they covered – Risk, Security, Risk & Security, or Security cost. With the frameworks we analysed how an enterprise may choose to map its security and risk needs for a complete security solution.

Lastly, we gathered relevant security and risk metrics that would support SOC personnel with quantitative risk assessment. Our research included articles from both scientific literature as well as standards used in practice. The collection of metrics points to a broad way of measuring security and risk impact and costs. We did find that some studies lacked empirical evaluation of metrics in their research, thus they should be used with caution. The security cost metrics were also found in the frameworks we came across, and we further explored more costs to complete our research in terms of effective countermeasure section. One form of cost associated with risk is loss, and according to FAIR, this can be primary loss or secondary loss based on which stakeholder is affected. Moreover, there is a cost associated with applying countermeasures to reduce the frequency and impact of a risk scenario. These were all considered when we defined metrics for input into the MORSE approach.

RQ 3: How can the business impact be measured for a security incident?

- **RQ 3a: Which metrics/KPIs can be defined, aligned with the types of impact?**

Once we concluded our literature survey, we started designing the artefact for this research where we answered this and subsequent research questions. Through this RQ, we also try to eliminate the gap in scientific literature relating to the business impact of security incidents relating with Enterprise Architecture. We find that the Open FAIR methodology provides a good basis for capturing quantitative business impact. In FAIR, there are 6 forms of losses defined which relate primary loss and secondary loss to a risk scenario. The impact is classified based on where the liability lies, i.e., if the primary stakeholder is affected or a repercussion from secondary stakeholders, like fines, reputation loss etc.

To capture the impact in MORSE, we defined several metrics and proposed formulae for calculations. The values of these metrics are taken as input in stage 2 – Risk identification in our approach and is done while carrying out the populating metrics task. The metrics which are defined here include exploitability, Loss Magnitude, Number of threat events, asset value and uncertainty. The metrics are defined at the element level, and by our use of ArchiMate modelling, these remain irrespective of which view or viewpoint the element is present in. Further we define the units in which risk is measured, which is ‘currency per year’. This is based on LEF in terms of loss events in a year and the LM which is in currency terms. The metrics are further explained in the Design chapter.

RQ 4: What factors influence the choice of control measures and incident response courses of action in an organization?

- **RQ 4a How to relate risk appetite to EA models?**
- **RQ 4b Can the elements in EA be related to these factors?**

For answering the next RQ, we described the risk evaluation and risk treatment stages in MORSE. We define the risk appetite on an organizational level as the amount of loss that the organization can withstand to pursue its strategic goals. Additionally, we define a risk tolerance at the organizational and at process level to indicate at a more granular level the acceptable risk. In the Stage 4, Risk evaluation, this value is checked with the calculated residual risk of the asset and displayed through a colour view in Enterprise Studio. After executing the algorithm, the asset is coloured red, green or blue depending on how it the risk compares to the defined values of risk appetite and risk tolerance.

To reduce the risk to an acceptable level, the risk manager would select appropriate control measures. We defined the metrics of – control strength, control measure cost and control measure type for each countermeasure. The control strength would define to what extent the risk is reduced by influencing the LEF or LM in a risk scenario, depending on the type of control. The control types are derived from Open FAIR with the addition of insurance type control. The risk manager has a portfolio view of controls to choose from but would also check the technical feasibility and capabilities of the SOC before applying them. The manager can also choose controls that define an incident response plan, which may be executed through a SOAR, that directs how to react when a loss scenario has occurred.

Further we proposed a ROSI function in which the manager would select an appropriate set of control measures for as many vulnerabilities as possible and try to optimize them. We have used ArchiMate modelling notation for EA, in which risk and security overlay has been proposed as specializations of existing elements which are reused in our approach.

RQ 5: How can we calculate a risk score in Enterprise Architecture models?

- **RQ 5a How does the risk score propagate in EA models?**

We had defined this question to see how EA can support risk modelling and benefit cyber security operations in organizations. We use industry-standard calculation of risk, which is a product of the probability of a loss scenario and the impact it causes. As we have used Open FAIR Risk Taxonomy, this is expressed as $Risk = LEF * LM$, given in equation 5.10. For arriving at this formula, the Loss Event Frequency is calculated using the Threat Event Frequencies, which in turn is a function of how many times an attack is likely to attack a given vulnerability and its probability of success. We have associated LEF with vulnerabilities and risk elements in the risk scenario. This is because a vulnerability can be exploited several times, but there are chances that it may not lead to a loss scenario if the adversary is not successful in reaching their target asset. This is expressed as the attack path in an attack graph visualized through MORSE. The Loss Magnitude is calculated as a sum of Primary Loss and Secondary loss in a risk scenario. Furthermore, the risk is presented as a range of values, which is defined by uncertainty in the input variables. This is done because it is almost impossible to accurately estimate the risk that would occur in the future.

For propagation of risk, we have proposed to model risk scenario through attack graphs. In this the vulnerabilities in the system are linked based on how an adversary would move within a secured enterprise. The probability of success is computed on relationship

using the proposed formulae which use the disjunctive and conjunctive properties to join vulnerabilities using logical operations of “AND” and “OR” relationship. These define the series of vulnerabilities an attacker would have to succeed in exploiting to reach their intended target.

RQ 6: What is an effective decision-making method in SOC that uses model-based security analysis?

- **RQ 6a How to select an appropriate control measure based on the risk score of the business concept?**

This research question is similar to **RQ 4**, but it dives into how the control measure selection is done as compared to what factors it is based on. This research question is also related to functional requirement **FR4** which we validated as partially fulfilled in the Demonstration chapter.

Through MORSE we are supporting SOC to make an effective decision on control measures selection based on the risk to an organization’s assets. Stage 5 – Risk treatment in our approach is developed for this purpose which includes four tasks that depend on the output of risk evaluation. Once the risk analyst has decided that controls need to be applied to bring the risk within the risk appetite, they can choose from a portfolio of control. We have defined a ROSI function that would refresh based on the controls selected for the risk scenario. The function is based on the control strength and the cost of controls. The analyst would check if it is technically feasible to apply a particular control before adding them to the attack graph. When a set of controls is selected for a risk scenario, the ROSI value, which is also displayed in the same view, is refreshed. This can be measured with a different set of control measures and the most optimum set can be selected.

RQ 7 How would this method benefit a SOC in practice?

This final research question was formulated to evaluate the proposed design in practice. We are unable to completely answer this question because the approach was not tested in a SOC and the expert opinion that we received were from professionals who did not have in-depth knowledge about the functioning of a SOC. However, from the evaluation workshop we have been able to answer several critical questions about the possible application of MORSE in practice.

A mini-workshop was conducted in which the 5 experts were introduced to the approach and asked to fill in a questionnaire based on the UTAUT model. We formulated eight questions to measure how well the MORSE approach would be accepted in a real-world setting and this is documented in the Evaluation chapter. The findings are generally positive and are summarized in Table 29. Two of the eight questions had a median score of 3, meaning participants neither agree nor disagree, and the rest of the questions had a median score of 4, which means the participants agree with it. The results suggest that the approach is not easy to use, because of the different skills needed and do not expect people in SOC to have modelling expertise. The participants also highlighted the lack of documentation regarding FAIR for end-users that could hamper risk assessment because of inadequate knowledge. Their opinion on MORSE leading to better selection of control measures was divided. The

experts, however, positively evaluated that the MORSE approach adequately captures the business impact of risk and the propagation of risk across different layers within an EA model.

Furthermore, we believe using our approach benefits an organization because they can have higher utilization of SOC applications by re-using functionality. This is covered in the Demonstration chapter where we showed how the controls available in an organization's portfolio to be re-used in a new risk scenario. Thus, providing greater coverage by security applications.

8.1. Limitations

There are some limitations in our research that are discussed here. One is that there is a considerable modelling effort required for effectively creating risk scenarios and giving accurate estimations for metric values. This is a known limitation with risk estimations that it is hard to predict what the losses would be or the probability of a malicious actor getting successful in their attempt. We have tried to use CVSS scores and provided some help to estimate in Table 14, but these cannot be accurate. Additionally, the MORSE approach uses CVSS v3 in the calculations. This score is updated with time, and if the approach is used in practice, the formula would also need to be updated if there are changes in the scoring method. This does create an external dependency.

One limitation that was also highlighted during the mini-workshop was about the sensitivity of the calculations to small variations in inputs. This requires further research to quantify the sensitivity of the scale, which could not be covered in this research.

Another limitation of the approach is that there is no loss magnitude associated with vulnerabilities. However different exploits can have different vulnerabilities in the same risk scenario. An example for this would be an attacker render a system unavailable thorough an exploit, while at the same time steal information from the corporate network. This would lead to multiple loss scenarios, which at present cannot be modelled in the approach.

For the evaluation of the artefact, we invited experts from BiZZdesign. The minimum experience with EA in the group was 12 years and maximum 20 years. However, one limitation was that the experts were not the end users of the artefact. The MORSE approach is intended to be used by Risk Managers and Risk Analysts in SOC, but these roles were not added in the evaluation workshop. This was because of the availability of participants at the company where this research is carried out. If there were more Risk analyst and Risk Managers participating then the evaluation could be more balanced. Another point regarding the evaluation is that the participants knew each other through the association of working in the same organization. We believe that this could lead to certain biases in opinion as the evaluation workshop was not anonymous.

One limitation is that the research is largely based on BiZZdesign Enterprise Studio and the features it offers. This was an opportunity to make use of the various features it offers as the research was carried out at BiZZdesign. However, the same features may not be available

in other modelling tools making this approach highly specific. This was not explored out as part of this research project because of the limited time and resources.

8.2. Contribution to scientific research

The contributions of this research to science are the combination of security-modelling using attack graphs with Enterprise Architecture. In our approach we can visualize the propagation of risk in EA models of organizations. This is a novel approach that the author has not seen done yet in published literature. Further this research uses quantitative risk assessment, using industry-standard Open FAIR methodology for calculating risk for different components in the architecture model. We have proposed several formulae in our artefact, e.g., probability of success, Loss Event Frequency, Loss Magnitude, Risk, ROSI, etc. which together are used to perform a complete risk assessment.

The literature review of this research is also beneficial to the scientific community as the author has not come across a similar study before. The systematic literature survey that combines knowledge from the fields of Enterprise Architecture, Information Security, and Risk Analysis by examining 29 articles. This resulted in the documentation of 10 risk analysis methods, 7 frameworks and 7 sets of metrics pertaining to the topics of interest. These 24 artefacts represent a way to assess security risk in organizations and can independently be used by other researchers.

Furthermore, this research relates the business aspects of organizations with the cybersecurity risk that they face. There is a known lack of research relating academic with practice, which our research combines, by using theoretical approaches, like attack graphs, with practical tools, like ISO standards, BiZZdesign Enterprise Studio and ArchiMate modelling language. This makes way for further research within this domain that would benefit both the scientific community and businesses looking to leverage this research.

8.3. Implications in practice

The core functionality MORSE offers to the organization that they can perform a quantitative risk assessment on their cyber security threat landscape. The result of the assessment is a numeric value that the business stakeholders can act upon. In traditional qualitative risk assessment approaches, the lack of a precise value would hinder quality decision-making by an impaired judgement of the severity of risk. With this approach, decision makers can clearly see what is the business impact of cyber risk to their assets and make informed investments to protect them.

The approach is based on industry standards like FAIR, ISO 31000, ISO27001, CVE etc. which are widely used in practice. Thus, in conjunction with this enterprise architecture modelling, organizations can leverage their existing resources to create value. Using the Open FAIR risk taxonomy, organizations can use standard terms like Loss Event Frequency, Loss Magnitude, Risk, etc. that have a consistent meaning with practitioners that would remove scenarios that are caused by misunderstanding and miscommunication.

We evaluated in Chapter 7 that MORSE can effectively calculate the Business impact of security risk. Organizations would find it useful to base their business decisions on this when making security investments. Additionally, the availability of cyber risk insurance in the risk treatment options, allows them to assess when planning a risk transfer strategy for treatment. The MORSE approach would ultimately lead to better communication of risk within the organization, from a security analyst in the SOC developing the risk scenario to executives who are making strategies regarding the enterprise's security posture.

Furthermore, through the risk monitoring phase of MORSE, the risk can be communicated effectively through the organization. This is an important aspect of risk management that the right stakeholders are kept informed. Through the demonstration in Chapter 6 we showed for our approach, we used the dashboard functionality in Enterprise Studio. This is one way of reporting risk transparently from the EA model of the organization. It is important that the outcomes of risk analysis are effectively communicated by applying objectives we elucidated in stage 6. By doing so, the decision makers can make fact-based decision on risk to improve the cybersecurity of their organization.

8.4. Future research

During this research we also noted some areas which could have been explored further, but due to the limited scope of the thesis project could not be covered. In this section we list these as future research areas.

Firstly, MORSE should be implemented on a larger model with multiple assets and risk. The current model is tested on a sample case, and does not equate to how it would perform when implemented in a large organization. It is expected that there would be modifications needed based on the real-world test results.

Next, the control measure strength is given as an input parameter from 1 to 10. However, there is a possibility to perform detailed analysis to arrive at the control strength. This is also going to benefit when a particular control can be realized by multiple applications in the SOC, and having separate control strengths, backed by analysis, would allow making an informed selection. An extension of FAIR called FAIR-CAM (Control Analytic Model) is stated to be launched in October 2021. It aims to evaluate quantified of benefit from controls in terms of risk reduction. This would allow security teams to empirically measure the efficacy of controls [76]. A whitepaper is expected to be published and as an enhancement to MORSE, we would recommend that to be investigated.

Further, in the Literature Review section we had identified additional articles, outside of SLR, to support our research. One of them was on attack graphs which are used in modelling techniques by Hacks et al. (2019) [52] and employ domain specific language. In future, we would like to look at possibilities to integrate our approach with Meta Attack Language they propose. This would allow for automated generation of attack trees and decrease effort in defining a risk scenario.

Additionally, as it was discussed during the workshop, the calculations could be enhanced by including Monte Carlo simulations and applying convolution. We would also keep this as future work, as it would allow the risk analysis to be more complete in terms of quantification of risk metric. Further a sensitivity analysis should be performed and the result be presented with a confidence score.

As the final research area, we would propose the productization of this approach within Enterprise Studio. Currently, the approach was demonstrated by creating a new model in ES. Once the approach is at a stage that it can be distributed at scale, we would propose to include it as an example within Enterprise Studio and allow the metric values to be pre-built within models. This way it can be quickly deployed as a new model. This should also be accompanied with training documentation which would allow practitioners to quickly get started with using the MORSE approach.

8.5. Recommendations

In the last section of this report, we report on our recommendations to organizations applying MORSE. A high degree of effort is required to complete a model-based security risk assessment; however, the expertise of the users varies significantly considering their skillset. The risk manager or analyst working on an assessment would require knowledge about Enterprise Architecture, ArchiMate modelling language, risk, and security. In addition, they must also be versed in applying security controls to applications so that they can assess the technical feasibility of a particular integration. This can however be improved if the risk assessment is done as a collaborative process. The analyst would involve different experts who can provide domain expertise, in software, security, risk, and EA modelling to cover the lack of skills that are required to carry out the assessment by a single person. Our recommendation here would be to train the users of MORSE with the necessary skills before performing risk assessment and define roles with different tasks. This would also include using a consistent vocabulary related to risk, like Open FAIR, within the organization to ensure clear communication.

Additionally, to build a large number of attack scenarios, penetration testing can be carried out so that known vulnerabilities are exposed. This way the organization can become aware of multiple points from where potential hackers can infiltrate and preventive measures can be placed. However, this still assumes that the business knows their weakness, which is not always clear and malicious actors would constantly be trying to find exploits. These can be released as 0-day exploits and organizations must be responsive to protect themselves from unknown attacks. One way to do this is by using subscription-based threat intelligence services.

Confidence in the results of the analysis is also an important aspect to consider as there can be significant security investment decisions that can be placed using the risk assessment. If the executives and managers have a high degree of confidence in the calculations, they would be willing to take important decisions based on the output of MORSE. This confidence must be built as the approach is used in practice. We would recommend that

several risk scenarios are modelled using MORSE and efficiency be measured using parameters deemed useful by the stakeholders.

As a generalization of MORSE, it may be applied to scenarios outside of cyber security. This is possible because we have used Open FAIR and ISO 31000 as the base, and these can theoretically be extended to risk scenarios in general. Thus, we would suggest if organizations embrace MORSE approach, they can also look at possibilities of applying it outside the context of cybersecurity for modelling other operational risk scenarios as well.

Appendix 1

Following the concept-centric technique by Webster and Watson (2002) [24], the concepts in Table 30 were identified for each paper in the literature review. These have been summarized in the 'Concepts' sub-section in the SLR Results section.

The 'y' in each of the cell in the table indicate that a particular concept (from the top row) was identified in that article.

Table 30 Concepts identified in articles

Paper ID	Title	Business	EA	Security	Risk	Analysis
Labadi et al. (2020) [35]	Petri Net-Based Approach for “cyber” Risks Modelling and Analysis for Industrial Systems				y	y
McClintock et al. (2020) [43]	Enterprise security architecture: Mythology or methodology?		y	y		y
Diefenbach et al. (2019) [41]	Towards an integration of information security management, risk management and enterprise architecture management - A literature review		y	y	y	y
Xiong et al. (2019) [32]	Re-using enterprise architecture repositories for agile threat modelling		y	y		y
Abbass (2019) [39]	ArchiMate based security risk assessment as a service: Preventing and responding to the cloud of things' risks		y		y	y
Mayer et al. (2019) [42]	An integrated conceptual model for information system security risk management supported by enterprise architecture management		y		y	y
Zhi et al. (2018) [36]	Quantitative evaluation in security assurance		y	y		y
Nather (2018) [40]	Improving information security through risk management and enterprise architecture integration		y		y	
Sousa et al. (2013) [27]	Assessing risks and opportunities in enterprise architecture using an extended adt approach		y		y	y
Sommestad et al. (2013) [77]	The cyber security modelling language: A tool for assessing the vulnerability of enterprise system architectures			y		y

Schiavone et al. (2013) [78]	Information security in enterprises - Ontology perspective			y		y
Burkett (2012) [79]	Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®		y	y		y
Schütte et al.(2012) [80]	Model-based security event management			y		
O-RA [37]	Risk Analysis (O-RA)				y	y
O-RA v2 [33]	Risk Analysis (O-RA), Version 2.0				y	y
O-RT v3 [13]	Risk Taxonomy (O-RT), Version 3.0				y	
de Castro et al. (2020) [34]	SCRAM: A Platform for Securely Measuring Cyber Risk. Harvard Data Science Review			y	y	
Granadillo et al. (2016) [38]	Selection of Mitigation Actions Based on Financial and Operational Impact Assessments	y		y		y
Böhme (2010) [44]	Security Metrics and Security Investment Models	y		y		
Anderson et al. (2019) [45]	Measuring the Changing Cost of Cybercrime	y				y
Kumar & Stoelinga (2017) [28]	Quantitative security and safety analysis with attack-fault trees			y		y
Jhavar et al. (2016) [26]	A Stochastic Framework for Quantitative Analysis of Attack-Defence Trees			y		y
Wang et al. (2020) [29]	A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model				y	y
Breu et al. (2008) [31]	Quantitative assessment of enterprise security system		y	y		y
Mukherjee & Mazumdar (2019) [46]	Security Concern' as a metric for enterprise business processes			y		y
Weintraub & Cohen (2018) [47]	Defining network exposure metrics in security risk scoring models			y		

Pereira & Santos (2014) [48]	Security metrics to evaluate organizational IT security	y		y		
Aissa et al. (2011) [49]	Defining and computing a value based cyber-security measure			y		y
Breier & Hudec (2011) [30]	Risk analysis supported by information security metrics			y	y	y

Appendix 2

The mini-workshop for the evaluation of this research was conducted on 15-July-2021. Following the workshop, a questionnaire was shared, and in this Appendix, we tabulate the data retrieved through the questionnaire. Participant profiles are tabulated in Table 27.

Table 31 Response Q1: The proposed approach is easy to use in practice.

Participant	Q1: Score	Q1: Positive opinion	Q1: Negative opinion
A	3	If you're experienced with modeling, it isn't very difficult	Many risk managers will not be experienced with models and the rigor needed for an approach like this. Moreover, the main issue in risk analysis is *identifying* possible vulnerabilities and attack vectors. The approach assumes these are already given.
B	3	Clear description of the steps and activities in each of the steps	Modeling experience required, assumes many input values, so there is a learning curve
C	4	A process driven approach is always an easy to understand way of working, end-users need to be 'guided' which this does	May need clearer labelling of 'artifacts' that are created at each stage to give better understanding
D	2	I believe in a model-based and well-structured approach.	But this may/will involve a lot of work, knowledge and expertise. Also because of the level of detail that may be required.
E	2	The approach provides a structured approach for quantifying security risk	I am not sure there is any way to do it that is easy in practice!

Table 32 Response Q2: The proposed approach is compatible with existing customer use cases for risk and security.

Participant	Q2: Score	Q2: Positive opinion	Q2: Negative opinion
A	3	-	Difficult to say, since "Risk" is such a broad topic
B	4	-	-
C	4	The underlying assets are indeed modelled in EA - and I don't think there is enough consideration in general EA practices on a standardised way of linking risk and security to what they do as their day job - sometimes an afterthought. This gives good visibility on the importance of getting it right as an in-parallel activity	This is still a relatively untapped area, where traditional 'EA' does not fully understand. More needs to be understood on the benefits.
D	-	-	-
E	4	The approach fits well as an extension to architecture activities.	The approach might be a lot to digest for security teams who are not currently working with modelling tools. This may be the biggest barrier to adoption.

Table 33 Response Q3: The proposed approach adequately captures business impact for a risk.

Participant	Q3: Score	Q3: Positive opinion	Q3: Negative opinion
A	3	-	Aggregate risk / total risk exposure is not simply the sum of all individual risks, since they may be correlated.
B	4	The used metrics are in business terms	As discussed, it could be made more explicit how to arrive at the business impact
C	4	Money money money, I think that is a good starting point	There may need to be more deep explanation on how we arrive at the impact values

D	4	I think when the method is applied correctly/completely, you are able to capture the business impact. The method provides the steps and ingredients that are needed for this.	The quantitative approach may give the idea that the presented outcomes are precise and correct. However, there may be a lot of uncertainty in the input values. The consequence/impact of this uncertainty should be clear and made (more) explicit.
E	4	The approach provides a structured way to quantify risk, and provide visibility to the business assets that are affected.	Need to consider how the sources of risk are connected with the impacted business assets (e.g. how to derive relationships) and how to best provide visibility of the assets affected by a risk.

Table 34 Response Q4: I would be able to find adequate knowledge and support about applying the approach in practice.

Participant	Q4: Score	Q4: Positive opinion	Q4: Negative opinion
A	3	I know the Open FAIR documents (and ArchiMate of course)	The Open FAIR standard isn't that well-documented from an end-user perspective
B	3	-	See response to first question: quite a lot of input needed, may be a challenge to find the right people to provide this
C	3	Good examples as illustration	Perhaps a little too basic in terms of example. Would likely need a full end-to-end explaining the approach and applying in practice
D	4	The approach is presented clearly. Based on its description I would be able to determine where my knowledge is lacking and where to look for more information.	-
E	3	This is an area where there is limited knowledge and skills in the market.	This is an area where there is limited knowledge and skills in the market.

Table 35 Response Q5: The approach captures the propagation of cyber risk effectively in Enterprise Architecture models.

Participant	Q5: Score	Q5: Positive opinion	Q5: Negative opinion
A	4	-	-
B	4	-	See response to business impact: propagation through EA models could be made more explicit
C	4	Key high level elements identified well.	Not 100% clear on the join-points between Risk and the underlying assets. How does the attack graph get populated? Since the assets are the things connected to vulnerabilities, how does that then connect to the Risk. Needs explanation.
D	4	The risk concepts are linked clearly to the ArchiMate concepts.	The use of an architecture model in deriving/defining attack-defence graphs may need more attention (as was also pointed out by Henk).
E	5	-	-

Table 36 Response Q6: The proposed approach would allow for better selection of control measures to mitigate risks.

Participant	Q6: Score	Q6: Positive opinion	Q6: Negative opinion
A	3	-	Better than what? I'm not sufficiently conversant with current approaches for this, not being a risk expert.
B	4	Making ROSI explicit should lead to a more well-founded selection of control measures	-
C	3	Reuse of existing standards - great approach, recommended	The process of going ahead to select measures maybe not detailed enough.

D	4	I think a model-based approach leads to a better identification (and possibly quantification) of risks. This enables also a better selection of measures.	-
E	4	If controls are modelled and related to the types of risks, threats and vulnerabilities they mitigate, then this approach will definitely help make the control selection process more efficient. But it does depend on the modelling / models being in place.	is there anything about modelling that can really improve the control selection approach? it is not really clear to me on this point.

Table 37 Response Q7: Applying the proposed risk quantification approach improves the ability to communicate about risk within an organization.

Participant	Q7: Score	Q7: Positive opinion	Q7: Negative opinion
A	4	The heatmaps are helpful	-
B	4	Good foundation for making risks and business impact explicit, can be used as the basis for more business-oriented visualizations	Other visualizations based on the information in the models may be needed for different stakeholders in the organization
C	3	Quantification is good - numbers speak volumes - and may possibly get 'technical' folks a seat at the exec table	In reality, how likely are EA practitioners (or any architects) really going to work with numbers related to impact of risk etc - may well be a separate team that handles that side, with EA more the 'consumers' and the 'joiners of dots'
D	3	It makes the discussion more concrete.	As said before, there may be a lot of uncertainty in the presented figures. This should be clear.
E	4	It should enable a better conversation with business stakeholders	-

Table 38 Response Q8: Using the proposed approach at a Security operations centre would lead to improved decision-making when responding to threats.

Participant	Q8: Score	Q8: Positive opinion	Q8: Negative opinion
A	3	-	Not sure, I'm not involved with SOCs.
B	4	-	-
C	4	It is the connection between all the assets which is the critical part here - if this can be stressed, then the decision-making benefits should be clear	As part of this, may need some 'samples' of decisions actually supported through this approach
D	4	I would expect so.	However, I'm not familiar with the current ways of working in SOCs.
E	4	It should enable better prioritisation of risks and risk treatments	I suspect some SOCs will see it as too much work to implement

References

- [1] World Economic Forum, "The Global Risks Report 2021," 2021. Accessed: 15-08-2021. [Online]. Available: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
- [2] J. Boehm, N. Curcio, P. Merrath, L. Shenton, and T. Stähle. "The risk-based approach to cybersecurity." McKinsey & Company. <https://www.mckinsey.com/business-functions/risk/our-insights/the-risk-based-approach-to-cybersecurity> (accessed 15-08-2021).
- [3] R. Wolthuis and F. Phillipson, "Quantifying Cyber security Risks," 2019, pp. 20-26.
- [4] D. Hubbard and D. Evans, "Problems with scoring methods and ordinal scales in risk assessment," *IBM J. Res. Dev.*, vol. 54, no. 3, pp. 246–255, 2010.
- [5] I. Band *et al.* "How to Model Enterprise Risk Management and Security with the ArchiMate® Language." <https://publications.opengroup.org/w172> (accessed 15-08-2021).
- [6] R. Wieringa, *Design Science Methodology for Information Systems and Software Engineering*. 2014, pp. 1-332.
- [7] M. A. Rood, "Enterprise architecture: definition, content, and utility," in *Proceedings of 3rd IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 17-19 April 1994 1994, pp. 106-111, doi: 10.1109/ENABL.1994.330494.
- [8] M. Lankhorst and H. v. Drunen, "Enterprise Architecture Development and Modelling Combining TOGAF and ArchiMate," 2007. [Online]. Available: <http://storage.ning.com/topology/rest/1.0/file/get/1696975678?profile=original>. [Online].
- [9] H. Jonkers *et al.*, "Towards a language for coherent enterprise architecture descriptions," in *Seventh IEEE International Enterprise Distributed Object Computing Conference, 2003. Proceedings.*, 19-19 Sept. 2003 2003, pp. 28-37, doi: 10.1109/EDOC.2003.1233835.
- [10] H. Jonkers, M. Lankhorst, R. V. Buuren, S. Hoppenbrouwer, M. Bonsangue, and L. V. D. Torre, "Concepts for Modeling Enterprise Architectures," *International Journal of Cooperative Information Systems*, vol. 13, no. 03, pp. 257-287, 2004, doi: 10.1142/s0218843004000985.
- [11] *ArchiMate® 3.1 Specification*, The Open Group, 2019. [Online]. Available: <https://pubs.opengroup.org/architecture/archimate3-doc/>
- [12] D. Basin, M. Clavel, and M. Egea, "A decade of model-driven security," presented at the Proceedings of the 16th ACM symposium on Access control models and

- technologies, Innsbruck, Austria, 2011. [Online]. Available: <https://doi.org/10.1145/1998441.1998443>.
- [13] *Risk Taxonomy 3.0*, The Open Group Standard, 2020.
- [14] H. Jonkers and D. A. C. Quartel, "Enterprise Architecture-Based Risk and Security Modelling and Analysis," in *Graphical Models for Security*, Cham, B. Kordy, M. Ekstedt, and D. S. Kim, Eds., 2016// 2016: Springer International Publishing, pp. 94-101.
- [15] *NEN-ISO 31000:2018 Risk management - Guidelines*, International Organization for Standardization, 2019.
- [16] International Organization for Standardization, "NEN-EN-ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements," 2017.
- [17] S. Mauw and M. Oostdijk, "Foundations of Attack Trees," in *Information Security and Cryptology - ICISC 2005*, Berlin, Heidelberg, D. H. Won and S. Kim, Eds., 2006// 2006: Springer Berlin Heidelberg, pp. 186-198.
- [18] C. L. Peter Firstbrook. "Innovation Insight for Extended Detection and Response." Gartner via FireEye. <https://content.fireeye.com/automated-defence/rpt-gartner-innovation-insight-for-xdr> (accessed 15-08-2021, 2021).
- [19] BiZZdesign Support. "Use of attributes versus metrics in modeling - BiZZdesign Support." <https://support.bizzdesign.com/display/knowledge/Use+of+attributes+versus+metrics+in+modeling> (accessed 15-08-2021).
- [20] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, pp. 45-77, 01/01 2007.
- [21] L. Bader, "IBM Sponsors the FAIR Institute to Advance Best Practices in Cyber Risk Management," ed, 2021.
- [22] Y. Xiao and M. Watson, "Guidance on Conducting a Systematic Literature Review," *Journal of Planning Education and Research*, vol. 39, no. 1, pp. 93-112, 2019, doi: 10.1177/0739456x17723971.
- [23] K. Barbara and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," vol. 2, 01/01 2007.
- [24] J. Webster and R. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Q.*, vol. 26, 2002.
- [25] A. Aldea, E. Vaicekauskaite, M. Daneva, and J. P. Sebastian Piest, "Assessing Resilience in Enterprise Architecture: A Systematic Review," in *Proceedings - 2020 IEEE 24th International Enterprise Distributed Object Computing Conference, EDOC 2020*, 2020, pp. 1-10, doi: 10.1109/EDOC49727.2020.00011. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0->

- [85096365558&doi=10.1109%2fEDOC49727.2020.00011&partnerID=40&md5=aa72f012289f69fc5c21168c736a9003](https://doi.org/10.1109/EDOC49727.2020.00011&partnerID=40&md5=aa72f012289f69fc5c21168c736a9003)
- [26] R. Jhawar, K. Lounis, and S. Mauw, "A Stochastic Framework for Quantitative Analysis of Attack-Defence Trees," in *Security and Trust Management*, Cham, G. Barthe, E. Markatos, and P. Samarati, Eds., 2016// 2016: Springer International Publishing, pp. 138-153.
- [27] S. Sousa, D. Marosin, K. Gaaloul, and N. Mayer, "Assessing risks and opportunities in enterprise architecture using an extended adt approach," 2013, pp. 81-90, doi: 10.1109/EDOC.2013.18. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84892546915&doi=10.1109%2fEDOC.2013.18&partnerID=40&md5=b92f40476b476384c35361cd5fcd84>
- [28] R. Kumar and M. Stoelinga, "Quantitative Security and Safety Analysis with Attack-Fault Trees," presented at the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), 2017.
- [29] J. Wang, M. Neil, and N. Fenton, "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model," *Computers & Security*, vol. 89, p. 101659, 2020/02/01/ 2020, doi: <https://doi.org/10.1016/j.cose.2019.101659>.
- [30] J. Breier and L. Hudec, "Risk analysis supported by information security metrics," presented at the Proceedings of the 12th International Conference on Computer Systems and Technologies, Vienna, Austria, 2011. [Online]. Available: <https://doi.org/10.1145/2023607.2023673>.
- [31] R. Breu, F. Innerhofer-Oberperfler, and A. Yautsiukhin, "Quantitative Assessment of Enterprise Security System," presented at the 2008 Third International Conference on Availability, Reliability and Security, 2008.
- [32] W. Xiong, P. Carlsson, and R. Lagerstrom, "Re-using enterprise architecture repositories for agile threat modeling," in *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, 2019, vol. 2019-October, pp. 118-127, doi: 10.1109/EDOCW.2019.00031. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075973320&doi=10.1109%2fEDOCW.2019.00031&partnerID=40&md5=a094dbf88d3132a806ad13716af56da9>
- [33] *Risk Analysis (O-RA), Version 2.0*, The Open Group Standard, 2020.
- [34] L. a. L. de Castro, Andrew W. and Reynolds, Taylor and Susan, Fransisca and Vaikuntanathan, Vinod and Weitzner, Daniel and Zhang, Nicolas, "SCRAM: A Platform for Securely Measuring Cyber Risk," *Harvard Data Science Review*, 2020-09-16 2020, doi: 10.1162/99608f92.b4bb506a.

- [35] K. Labadi, A. M. Darcherif, I. El Abbassi, and S. Hamaci, "Petri Net-Based Approach for "cyber" Risks Modelling and Analysis for Industrial Systems," in *E3S Web of Conferences*, 2020, vol. 170, doi: 10.1051/e3sconf/202017002001. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85088475298&doi=10.1051%2fe3sconf%2f202017002001&partnerID=40&md5=3fcf720e2f2f57730c7e4e8d37d41d5f>
- [36] Q. Zhi, S. Yamamoto, and S. Morisaki, "Quantitative evaluation in security assurance," in *2018 IEEE 4th International Conference on Computer and Communications, ICC3 2018*, 2018, pp. 2477-2483, doi: 10.1109/CompComm.2018.8780877. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85070812299&doi=10.1109%2fCompComm.2018.8780877&partnerID=40&md5=dc4021c392a0dc81b785b5a97e6d1279>
- [37] *Risk Analysis (O-RA)*, The Open Group Standard, 2013.
- [38] G. G. Granadillo, A. Motzek, J. Garcia-Alfaro, and H. Debar, "Selection of Mitigation Actions Based on Financial and Operational Impact Assessments," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 31 Aug.-2 Sept. 2016 2016, pp. 137-146, doi: 10.1109/ARES.2016.3.
- [39] W. Abbass, A. Baina, and M. Bellafkih, "ArchiMate based security risk assessment as a service: Preventing and responding to the cloud of things' risks," 2019, doi: 10.1109/WINCOM47513.2019.8942475. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078102213&doi=10.1109%2fWINCOM47513.2019.8942475&partnerID=40&md5=42c9a86249c4c60dfab66cec09dc530f>
- [40] S. Nather, "Improving information security through risk management and enterprise architecture integration," 2018, vol. 2018-March, pp. 420-426. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051720425&partnerID=40&md5=42bf48232728f10e2a0da6195ba4f137>. [Online].
- [41] T. Diefenbach, C. Lucke, and U. Lechner, "Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management – A Literature Review," presented at the 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2019.
- [42] N. Mayer, J. Aubert, E. Grandry, and C. Feltus. *An integrated conceptual model for information system security risk management and enterprise architecture management based on TOGAF*, *Lecture Notes in Business Information Processing*, vol. 267, pp. 353-361, 2016.
- [43] M. McClintock, K. Falkner, C. Szabo, and Y. Yarom, "Enterprise security architecture: Mythology or methodology?," in *ICEIS 2020 - Proceedings of the*

- 22nd International Conference on Enterprise Information Systems, 2020, vol. 2, pp. 679-689. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091400522&partnerID=40&md5=8fd5fa8b6f446a2e3cfd1fba1cf13578>. [Online].
- [44] R. Böhme, "Security Metrics and Security Investment Models," in *Advances in Information and Computer Security*, Berlin, Heidelberg, I. Echizen, N. Kunihiko, and R. Sasaki, Eds., 2010// 2010: Springer Berlin Heidelberg, pp. 10-24.
- [45] R. Anderson *et al.*, "Measuring the changing cost of cybercrime," 2019.
- [46] P. Mukherjee and C. Mazumdar, "'Security Concern' as a Metric for Enterprise Business Processes," *IEEE Systems Journal*, vol. 13, no. 4, pp. 4015-4026, 2019, doi: 10.1109/JSYST.2019.2918116.
- [47] E. Weintraub and Y. Cohen, "Defining Network Exposure Metrics in Security Risk Scoring Models," *International Journal of Advanced Computer Science and Applications*, vol. 9, 2018.
- [48] T. Pereira and H. Santos, "Security metrics to evaluate organizational IT security," presented at the Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance, Guimaraes, Portugal, 2014. [Online]. Available: <https://doi.org/10.1145/2691195.2691275>.
- [49] A. Aissa, R. Abercrombie, and F. T. Sheldon, "Defining and computing a value based cyber-security measure," *Information Systems and e-Business Management*, vol. online, pp. 1-21, 04/05 2011, doi: 10.1007/s10257-011-0177-1.
- [50] F. Innerhofer-Oberperfler and R. Brey, *Using an Enterprise Architecture for IT Risk Management*. 2006, pp. 1-12.
- [51] A. Le, Y. Chen, K. K. Chai, A. Vasenev, and L. Montoya, "Incorporating FAIR into Bayesian Network for Numerical Assessment of Loss Event Frequencies of Smart Grid Cyber Threats," *Mobile Networks and Applications*, vol. 24, no. 5, pp. 1713-1721, 2019/10/01 2019, doi: 10.1007/s11036-018-1047-6.
- [52] S. Hacks, A. Hacks, S. Katsikeas, B. Klaer, and R. Lagerstrom, "Creating meta attack language instances using archimate: Applied to electric power and energy system cases," in *Proceedings - 2019 IEEE 23rd International Enterprise Distributed Object Computing Conference, EDOC 2019*, 2019, pp. 88-97, doi: 10.1109/EDOC.2019.00020. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85078238227&doi=10.1109%2fEDOC.2019.00020&partnerID=40&md5=2da57c5c fb0d86cb98af601c8c6775f7>
- [53] P. Johnson, R. Lagerström, and M. Ekstedt, "A Meta Language for Threat Modeling and Attack Simulations," presented at the Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 2018. [Online]. Available: <https://doi.org/10.1145/3230833.3232799>.

- [54] *ISO/IEC 27005 - Information technology - Security techniques - Information security risk management*, International Organization for Standardization, 2018.
- [55] BiZZdesign Support. "Use of risk and security-related elements in an ERSM modeling process - BiZZdesign Support." <https://support.bizzdesign.com/display/knowledge/Use+of+risk+and+security-related+elements+in+an+ERSM+modeling+process> (accessed 15-08-2021, 2021).
- [56] T. Suarez. "A Crash Course on Capturing Loss Magnitude with the FAIR Model." <https://www.fairinstitute.org/blog/a-crash-course-on-capturing-loss-magnitude-with-the-fair-model> (accessed 15-08-2021).
- [57] M. U. Aksu *et al.*, "A quantitative CVSS-based cyber security risk assessment methodology for IT systems," in *2017 International Carnahan Conference on Security Technology (ICCST)*, 23-26 Oct. 2017 2017, pp. 1-8, doi: 10.1109/CCST.2017.8167819.
- [58] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61-74, 2012, doi: 10.1109/TDSC.2011.34.
- [59] Forum of Incident Response and Security Teams (FIRST). "Common Vulnerability Scoring System v3.1: Specification Document." <https://www.first.org/cvss/v3.1/specification-document> (accessed 05-07-2021, 2021).
- [60] M. Ekstedt and T. Sommestad, "Enterprise Architecture Models for Cyber Security Analysis," pp. 1-6, 2009.
- [61] O. Gadyatskaya, C. Harpes, S. Mauw, C. Muller, and S. Muller, "Bridging Two Worlds: Reconciling Practical Risk Assessment Methodologies with Theory of Attack Trees," Cham, 2016: Springer International Publishing, in *Graphical Models for Security*, pp. 80-93.
- [62] S. Muller, C. Harpes, and C. Muller, "Fast and Optimal Countermeasure Selection for Attack Defence Trees," (in English), *Lect Notes Comput Sc*, vol. 10224, pp. 53-65, 2017, doi: 10.1007/978-3-319-57858-3_5.
- [63] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438-457, 2002, doi: 10.1145/581271.581274.
- [64] M. Simos. "Microsoft Cybersecurity Reference Architectures." Microsoft <https://aka.ms/MCRA> (accessed 15-08-2021, 2021).
- [65] B. Support. "Enterprise Portfolio Management - BiZZdesign Support." <https://support.bizzdesign.com/display/knowledge/Enterprise+Portfolio+Management> (accessed 15-08-2021).

- [66] I. Yevseyeva, V. B. Fernandes, A. van Moorsel, H. Janicke, and M. Emmerich, "Two-stage Security Controls Selection," *Procedia Computer Science*, vol. 100, pp. 971-978, 2016/01/01/ 2016, doi: <https://doi.org/10.1016/j.procs.2016.09.261>.
- [67] I. Yevseyeva, V. Basto-Fernandes, M. Emmerich, and A. van Moorsel, "Selecting Optimal Subset of Security Controls," *Procedia Computer Science*, vol. 64, pp. 1035-1042, 2015/01/01/ 2015, doi: <https://doi.org/10.1016/j.procs.2015.08.625>.
- [68] W. Sonnenreich, J. Albanese, and B. Stout, "Return On Security Investment (ROSI) - A Practical Quantitative Modell," *J. Res. Pract. Inf. Technol.*, vol. 38, 2006.
- [69] Jim Boehm, James M. Kaplan, Peter Merrath, Thomas Poppensieker, and T. Stähle. "Enhanced cyberrisk reporting: Opening doors to risk-based cybersecurity." <https://www.mckinsey.com/business-functions/risk/our-insights/enhanced-cyberrisk-reporting-opening-doors-to-risk-based-cybersecurity> (accessed 15-08-2021).
- [70] V. Egle, "Development of a method to implement the concepts of resilience in EA," ed, 2020.
- [71] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, vol. 27, no. 3, pp. 425-478, 2003, doi: 10.2307/30036540.
- [72] I. E. Allen and C. A. Seaman, "Likert scales and data analyses," *Quality progress*, vol. 40, no. 7, pp. 64-65, 2007.
- [73] J. Fernando. "Return on Investment (ROI)." <https://www.investopedia.com/terms/r/returnoninvestment.asp> (accessed 15-08-2021).
- [74] European Network and Information Security Agency (ENISA). "Introduction to Return on Security Investment." https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport (accessed 15-08-2021).
- [75] C. Onwubiko and A. Onwubiko, "Cyber KPI for Return on Security Investment," in *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 3-4 June 2019 2019, pp. 1-8, doi: 10.1109/CyberSA.2019.8899375.
- [76] J. B. Copeland, "Jack Jones Previews the FAIR Controls Analytics Model (FAIR-CAM) at the 2021 RSA Conference," vol. 2021, ed, 2021.
- [77] T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal*, Article vol. 7, no. 3, pp. 363-373, 2013, Art no. 6378394, doi: 10.1109/JSYST.2012.2221853.
- [78] S. Schiavone, L. Garg, and K. Summers, "Information security in enterprises - Ontology perspective," in *7th European Conference on Information Management*

- and Evaluation, ECIME 2013*, 2013, pp. 164-173. [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84893616137&partnerID=40&md5=55a995fcf409baaa28e971ce73457b4d>.
- [79] J. S. Burkett, "Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA[®]," *Information Security Journal*, Article vol. 21, no. 1, pp. 47-54, 2012, doi: 10.1080/19393555.2011.629341.
- [80] J. Schütte, R. Rieke, and T. Winkelvos. *Model-based security event management, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 7531 LNCS, pp. 181-190, 2012.