Universiteit Leiden

ICT in Business and the Public Sector

Bridging the gap between risk assessment and security operations

Name: Jari Egberts
Student-no: 2470179

Date: 28-07-2021

1st supervisor: Olga Gadyatskaya
2nd supervisor: Christoph Stettina

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Acknowledgement

Everything comes to an end, including my study at the University Leiden. It has been an inspiring and valuable time. I want to thank everyone that has contributed to my learning process.

Foremost, I want to thank my first supervisor Olga Gadyatskaya for her motivation and outstanding support throughout the thesis project, answering questions, having patience, providing feedback and advice when needed.

Another acknowledgement goes to my second supervisor Dr C. J. (Christoph) Stettina for providing valuable insights and feedback.

I also want to thank Talitha Papelard for the monitoring and support throughout the process, including the extensive knowledge about the topic and providing me the environment to do the research.

In addition, I want to thank my research participants for contributing to my research by helping me to gather data and valuable insights about the topic.

Finally, I want to thank my family and girlfriend for their motivation, encouragement, and support during my thesis project.

Jari Egberts

July 28th, 2021

Abstract

Background. Due to the rise of the internet and digitalization more cyber threats can occur. To be prepared for potential attacks risk assessment and security operations are necessary to provide response capabilities. The first respondents (monitoring and detection) performing the security operations are different people from the ones that participate in the risk assessment and threat modeling (risk managers and security developers). Therefore, there might be challenges in communication and information sharing between risk assessment and security operation teams.

Objective. The objective of this thesis is to research the information exchange and communication channels between the risk and threat modelers and security operations. This will lead to an insight into the communication, information needs and what information is being exchanged (problem / gap description).

Method. Exploratory research is used to research the gap between risk assessment and security operations. Eleven interviews are conducted using semi-structured interviews. To analyze the qualitative data set, an approach based on the Grounded Theory is used.

Results. By conducting the literature review and the interviews, we have identified the gap between risk assessment and security operations. We have proposed guidelines and have built a model to improve the information exchange, so that both planners (risk managers and security developers) and first respondents are supported in their activities.

Conclusion. Based on the research, we can say that the gap between risk assessment and security operations is the result of a different orientation of both exercises. Risk assessment focusses more on the business, and security operations more on the technical components. This results in a knowledge gap and different languages, which creates difficulties for translating risks and threats into a technical solution. To bridge the gap, joint exercises can be done to create a common understanding between the two and to identify the information needs.

Keywords: Risk assessment, security operations, security monitoring, SIEM, use-cases, information exchange.

Table of Contents

List of Figures

List of Tables

Introduction

Digital technology is becoming increasingly involved in our daily lives. These digital technologies are replacing human decision-based tasks, for example, driving and decision-making. We are becoming more reliant upon digital infrastructures (CyBOK, 2019). However, due to the digitalization, globalization, and the rise of the internet more cyber threats can occur and the digital infrastructures can be disrupted indiscriminately. The prevention and response to these threats and attacks are part of cybersecurity. Therefore, cyber security risk management and assessment is an important activity to mitigate risks and prevent attacks.

1.1 Problem statement

An essential part of cybersecurity management includes the process of managing incidents and rapidly responding to cyber-attacks (CyBOK, 2019). To do this, risk assessment and threat modeling are necessary to identify, assess and control risks and threats to an organization. The results of risk assessment and threat modeling are communicated to various levels of management who make decisions appropriate to the level of security for the organization, for example, security operations (first respondents). The first respondents are the ones that must act when an actual attack occurs.

The first respondents (monitoring and detection) performing the security operations are different people from the ones that participate in the risk assessment and threat modeling (risk managers and security developers). Therefore, there might be challenges in communication and information sharing between risk assessment and security operation teams. This can result in miscommunication among teams and the possibility that the security operations center (SOC) will not have enough information about the envisaged threat scenarios. The people that participate in the risk assessment and threat modeling should provide information about the different risks and threats in such a way that security operations can implement controls and use-cases in order to be able to monitor these threats and to react if an actual attack occurs.

We posit that by using the information from the risk assessment and threat modeling in a structured way, a potential increase in effectivity, efficiency (less resources) and security level could be achieved. Also, security operations can adequately mitigate the risks identified by the risk analysts.

1.2 Research gap

There exists a large body of works on how to perform risk assessment and threat modeling to define, analyze, communicate, and mitigate risks, and on how to identify vulnerabilities. In addition, there are related studies to this research about the gap between risk assessment and security operations.

A study performed by (Osório, 2018) also stated that there is a gap between the SOC team and the business managers regarding the communication of security risk. The objective of this study is to bridge this gap by conceiving and implementing a SIEM (Security information and event management) extension to assess risk hierarchically. In this context, a framework has been developed. The framework uses information coming from the SIEM and adds the results of the risk assessment to it. Another study performed by (dos Santos Vilar Ferreira, 2017), developed a multi-level model for risk assessment in SIEM and created a tool to implement this model. The model is divided into three layers: hosts, applications, and services. Each of these layers has a different perspective. The risk assessment is done based on the assessment of vulnerabilities severity, the risk of dependencies, and incidents severity that each asset has.

However, these studies focus on proposing new solutions in the form of new tools, SIEM systems and risk managements systems, while not investigating how to improve the current practices and systems in organizations. Many organizations are not able to afford switching to new solutions.

Also, the literature and studies do not contain a specific prescription, to the best of our knowledge, to communicate the results from risk assessment and threat modeling to security operations including the information that is needed to implement a monitoring solution.

1.3 Research objective

The objective of this thesis is to research the information exchange and communication channels between the risk and threat modelers and security operations. This will lead into an insight into the communication, information needs and what information is being exchanged (problem / gap description). To improve the gap possible improvements will be identified

(proposal) to support both planners (risk managers and security developers) and first respondents in their activities.

1.4 Research scope

The research focuses on organizations that provide security services to their clients in the form of cyber risk management and security operations. Risk assessment and threat modeling are needed beforehand to identify potential risks and threats for clients so that the organization is able to provide security controls or monitoring / detection to reduce client specific risks.

1.5 Research questions

To achieve the earlier described research objective, we have defined the following research questions and its sub questions:

RQ1: "What is the gap between risk assessment and security operations and how could this be improved?"

SQ1: "How is the information exchange organized according to the methods and best practices in security risk management, threat modeling and security operations?"

SQ2: "What is missing in the information exchange between risk assessment / threat modeling and security operations?"

SQ3: "What process or guidelines can be implemented to improve the information exchange between risk assessment / threat modeling and security operations?"

1.6 Key definitions

For this thesis, there are a couple of concepts that underpin the subject of risk assessment and threat modeling. For these concepts we have agreed on the following definitions:

Concept	Definition
Risk	"Risk is a likelihood of potential for harm from a cyber attack. The commonly used formula is the probability of a threat attacking multiplied by the probability of a vulnerability be present multiplied by the size of the impact if the attack is successful" (Edgar & Manz, 2017).
Threat	"A threat is any deliberate source of potential damage or danger. In cyber space, damage from threats is adverse impacts to the operation of a system or the resources, including data, of a system" (Edgar & Manz, 2017).
Control	"Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be administrative, technical, management, or legal in nature" (CyBOK, 2019).
Vulnerability	"A vulnerability is weakness in a system, either by design, configuration, or process, that renders it open to exploitation by a given threat or susceptible to a given hazard" (Edgar & Manz, 2017).
Risk assessment	"Identification and, if possible, estimation of hazard; assessment of exposure and/or vulnerability; and estimation of risk, combining the likelihood and severity" (CyBOK, 2019).
Threat modeling	"Structured approach to identify, quantify and address the security risk associated with an application. It identifies the potential risks and vulnerabilities which are exploitable across targets but from an attacker's viewpoint" (Maheshwari, V., & Prasanna, 2017).
Risk management	"Risk management focuses on how to measure and quantify a state of cyber security. This includes quantifying the value of cyber security to an operation, how much of a threat is the operation

	exposed to, and scoring how mitigations and security controls affect the overall operational risk" (Edgar & Manz, 2017).

Table 1: Definitions

1.7 Research approach

We conduct the following steps to answer the research questions:

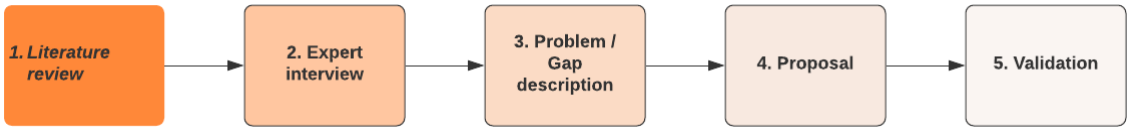

Figure 1: Research approach

Step	Description	Research question(s)
Literature review	A literature review will be conducted to review the concepts risk assessment, threat modeling and security operations in the scientific literature, industry standards and frameworks to identify the interrelationship between them. In addition, existing literature about the communication of risk assessment / threat modeling results will be analyzed to see what has been previously written about the topic.	**SQ1**: "How is the information exchange organized according to the methods and best practices in security risk management, threat modeling and security operations?"
Expert interview	After the literature review in-depth interviews with practitioners from different companies will be conducted to compare the literature with interview results and to get insights into the information needs / gaps / and possible	**SQ1**: "How is the information exchange organized according to the methods and best practices in security risk

	improvements. The practitioners are risk modelers, risk managers, security designers, security operations managers and security analysts. They have been selected to gather insights from both sides (risk assessment and security operations).	management, threat modeling and security operations?"
Problem / Gap description	Based on the literature review and the results of the interviews we can identify and describe the gap and possible bottlenecks / problems. The transcripts of the interviews will be analyzed to describe the gap and to develop the proposal. The Grounded theory approach will be used to build the theory by interpreting and understanding the broad patterns visible in the data that were collected through interviews at the different companies. This was done to describe the gap and determine what was missing in the information exchange.	**SQ2**: "What is missing in the information exchange between risk assessment / threat modeling and security operations?"
Proposal	To bridge the gap and improve the information exchange a proposal will be established based on the problem description, literature review and results of the interviews. • General improvements General guidelines on how to improve the gap. • Model / process	**SQ3**: "What process or guidelines can be implemented to improve the information exchange between risk assessment / threat modeling and security operations?"

	The model / process will describe what information must be exchanged through certain steps between risk assessment and security operations to improve the information exchange and gap.	
Validation	By using a questionnaire, we will validate this proposal with practitioners to see if the proposal is practical, realistic and if there are any limitations.	-

Table 2: Research approach

1.8 Thesis structure

The thesis will be structured as follows:

Chapter 2: Literature review

Conceptual foundation that will set the knowledge base for this research.

Chapter 3: Method

In the research methodology we will address the method adopted in this research.

Chapter 4: Results

The results chapter will contain the results of executing the research methods. As was previously described, this will contain a problem description and proposal based on the literature review and interviews.

Chapter 5: Discussion

In the discussion we will describe the significance of the results considering what is already known about the research problem being investigated.

Chapter 5: Conclusion

In the conclusion we will unite the findings in the thesis. This will be done by summarizing the main findings and suggesting opportunities for further research.

Literature review

In this section we introduce and define the core concepts of this study (risk management / assessment, threat modeling and security operations) for a conceptual foundation and a common understanding of the topics. Another goal is to establish what has already been examined in literature regarding the research questions by finding relevant research papers or industry best practices that are focused on the information exchange, or to establish that this topic has not been yet investigated in literature.

There is plenty of literature available about risk management, risk assessment, threat modeling and security operations. However, to the best of our knowledge, there is no specific literature available that specifies how the information exchange from the mapping exercises (risk assessment / threat modeling) to security operations should be organized in terms of needs, steps, or format.

There are standards and frameworks describing risk information sharing in more general term, which we will discuss them in section 2.3. For this thesis it is important to see how these methods communicate the results to decision makers and if there is specific communication with the SOC (security operations). Thus, we will have a look at the different frameworks that are available for risk assessment and threat modeling to see if they prescribe information about the communication and information exchange with security operations.

During the literature review we will answer the following sub questions:

SQ1: "How is the information exchange organized according to the methods and best practices in security risk management, threat modeling and security operations?"

In the first sections the different concepts will be described to observe the interrelationship between them. This is needed to describe the different responsibilities, needs and activities to understand the gap. After we introduced the concepts, an overview of the best practices for risk management, risk assessment and threat modeling will be given, including if they specify the communication and information exchange with security operations. This will provide an insight into the results of risk assessments and threat modeling, including the activities of the

security designer and risk managers. In the end we will form a conclusion to summarize the key findings of the literature review.

To find various scientific literature we have used Google Scholar and knowledge bases (CyBOK / NIST / MITRE). The Cyber Security Body of Knowledge's (CyBOK) purpose is to codify the cyber security knowledge, which underpins the profession. NIST develops cybersecurity standards, guidelines, best practices for the U.S. industry, federal agencies, and the broader public. MITRE provides standardized languages for communicating cybersecurity information and defining proper use of cybersecurity concepts (MITRE, 2018).

The main search criteria and keywords used to access these repositories were: cybersecurity, risk assessment, threat modeling, cyber security operations, best practices risk assessment, threat intelligence, threat communication, cyber risk interaction, and gap threat modeling security operations.

2.1 Risk management and risk assessment

In this section the concepts of risk management and risk assessment and trends / challenges will be described. First a definition will be given and later the overall process including the relationship between the concepts will be explained.

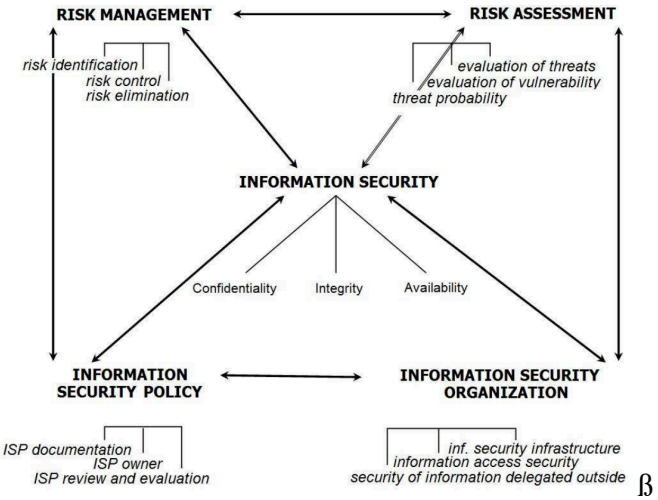

Figure 2: Aspects of information security management (Zawiła-Niedźwiecki & Byczkowski, 2009)

Risk management and risk assessment are both part of information security management with their own role. Risk management and risk assessment are interrelated; cybersecurity risk

assessment (referred to as “risk assessment”) is an integral part of an organization’s enterprise risk management process. According to (NIST, 2011), risk management can be described as consisting of four component processes: risk framing, risk assessment, risk response, and risk monitoring.

In the field of cyber risk management, a specific challenge and trend is the continuous change of traditional business models to digitally dependent business models. The shift from conventional business models to modern, more complicated, and interconnected internet-based business models has an impact on data privacy vulnerabilities and will increase the need for cyber risk management (Kosub, 2015). In addition, security and risk managers state that one of their biggest challenges is effectively communicating with business leaders. Writing risk appetite statements in business language engages business leaders by demonstrating the impact of risk policies. For example, by demonstrating how taking on too much risk might harm their interests or how being overly risk-averse can lead to missing opportunities (Gutierrez, 2021).

Risk assessment

ISO/IEC 27005:2011 describes that risk assessment: “Determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment”.

To perform risk assessment, the following activities should be executed: risk identification, risk analysis and risk evaluation. NIST (2012) describes that: “Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities”. Part of the risk assessment is to understand the applicable threats, including organization-specific threats. Monitoring and response activities can be implemented by conducting regular risk assessments that identify critical resources (NIST, 2012). The aim of risk assessment is to answer the following three questions (Kaplan and Garrick, 1981):

- What can go wrong?
- What is the likelihood that it will go wrong?
- What are the consequences if it goes wrong?

The questions mentioned above questions are translated into the table below:

E-mail system			
Threat	**Impact**	**Probability**	**Risk score**
Disclosure of confidential data	5	1	5

Figure 3: Risk assessment example

Impact = Max of (confidentiality, integrity, availability)
Probability = Measurement on how likely it is that the particular threat will occur.

Risk management

CyBOK (2019) describes risk management as "The process of developing and evaluating options to address the risks in a manner that is agreeable to people whose values may be impacted, bearing in mind agreement on how to address risk may involve a spectrum of (in)tolerance, from acceptance to rejection. It involves reviewing the information collected as part of the risk assessments. This information forms the basis of decisions leading to the outcomes for each perceived risk."

Risk management tries to answer the following questions based on the results of the risk assessment (Chittester and Haimes, 2004):

- What are the possibilities and what options are available?
- What are the associated trade-offs in terms of all costs, benefits, and risks?
- What is the impact of the current management decisions on future options?

To perform risk management, there are many methods available and in use to this day. The aim of these risk management frameworks and methods is to assist an organization in managing its risk exposures effectively by applying risk management process at various levels within of the organization (Ghazouani et al., 2014).

Part of the risk management process is to review the collected information from the risk assessment. Based on this information, the decision makers can decide on three possible outcomes for each risk (CyBOK, 2019):

Intolerable: When a risk is "intolerable", the system at risk needs to be abandoned or replaced. If this is not possible, vulnerabilities need to be reduced and exposure limited.

Tolerable: When a risk is "tolerable", the risk is reduced with reasonable and appropriate methods to a level as low as reasonably possible and reasonably allowable, for example by mitigating, sharing, or transferring risk. This depends on the risk appetite of the organization.

Acceptable: When a risk is "acceptable", risk reduction is not necessary and can proceed without intervention.

2.2 Threat modeling

To determine risk, a key step is to identify threat events that contribute to the likelihood and impact of risk. CSA Singapore (2021) describes that threat modeling helps owners to comprehensively identify threat events that are relevant to a system or application, so that they can focus on implementing effective control measures to protect key components within the system. The potential risks and vulnerabilities are identified from an attacker's viewpoint.

Threat modeling complements the risk assessment process by generating threat events with a detailed description of the actions, activities, and scenarios that the attacker can take to compromise the system. By integrating these threat events during the process, risk assessments will be made more rigorous and robust, resulting in in more targeted controls and effective layered defenses (CSA Singapore, 2021). Some approaches to perform threat modeling are implicitly or explicitly included in risk management / assessment approaches (MITRE, 2018). Threat modeling can therefore be considered as a sub-part of cybersecurity risk assessment or rather one of the steps (see Figure 4).

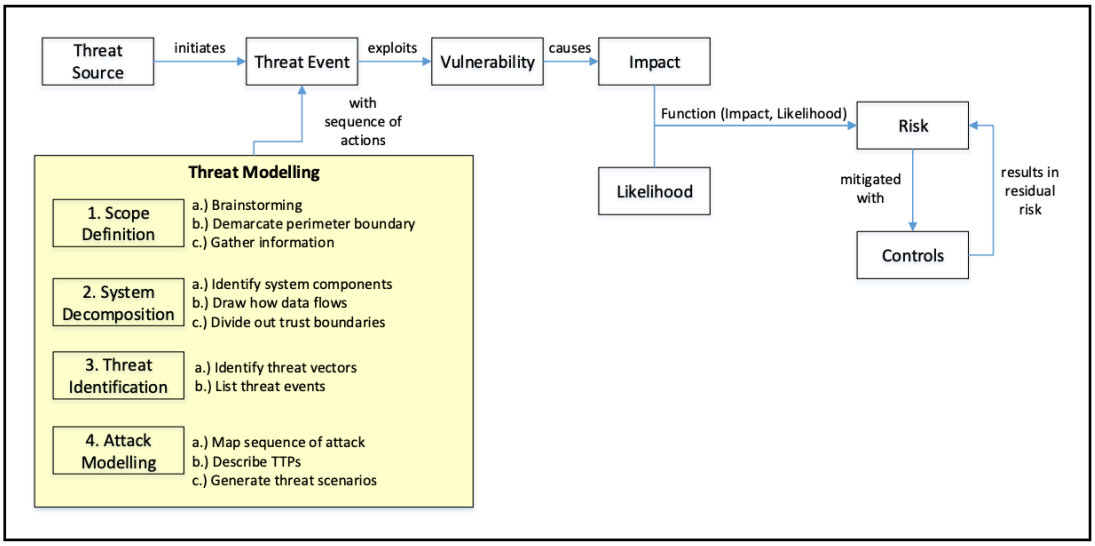

Figure 4: How Threat modeling Fits into Risk Assessment (CSA Singapore, 2021)

There are different directions on how threat modeling can be approached. The first approach is to model the threat first and then apply it to a relevant environment. The second approach is to model the system(s), data, and boundaries first and then determine what threats are relevant. The last approach is to identify the organization's assets first that could be affected by the threats. By applying any of these approaches to threat modeling, risk is estimated by assessing identified threat events or scenarios in terms of likelihood of occurrence and severity of impact. In order to address these threats, additional controls can be implemented (MITRE, 2018).

Thus, threat modeling is proactive, but it tries to anticipate the actual attacks that can take place. If an actual attack occurs, this knowledge about potential threats can be essential for the security operations and monitoring team when detective and reactive controls need to be implemented.

2.3 Methods / frameworks for risk management, risk assessment and threat modeling

For risk management, risk assessment and threat modeling there are a range of methods available. Some of these methods are international standards that provides guidelines on how transform vulnerability, threat, probability, and impact into a list in order to be able to prioritize and threat them (CyBOK, 2019).

There are different studies that compare different risk managements, risk assessments, and threat modeling frameworks and methods to identify their different characteristics. (Ghazouani et al., 2014) studied different methodologies for risk assessment to propose a mathematical formulation of risk that uses a lower level of granularity of its elements. Ionita (2013) conducted a survey that was aimed at uncovering the differences and limitations of the most common Risk Assessment frameworks and the conceptual models that support them, as well as the tools that implement them. MITRE (2018) conducted a survey of cyber threat modeling frameworks, presenting a comparative assessment of the surveyed frameworks. CyBOK (2019) performed an analysis regarding different risk assessment and management methods, providing a comparison table to enable selection based on the organizational and technical differences for each of the methods. For more information about the framework and methods, these studies can be consulted.

During the following section, the most common frameworks / methods in practice for risk management and risk assessment will be described to see if they prescribe information about the communication and information exchange with security operations. This is examined to answer the following question:

SQ1: "How is the information exchange organized according to the methods and best practices in security risk management, threat modeling and security operations?"

NIST SP-800-30 Risk Assessment Process

The US Government NIST guidelines (NIST, 2012) provide a cycle for conducting risk assessment by conducting the following steps: prepare (pre-assessment), conduct (appraisal and characterize), communicate (cross-cutting), and maintain (management).

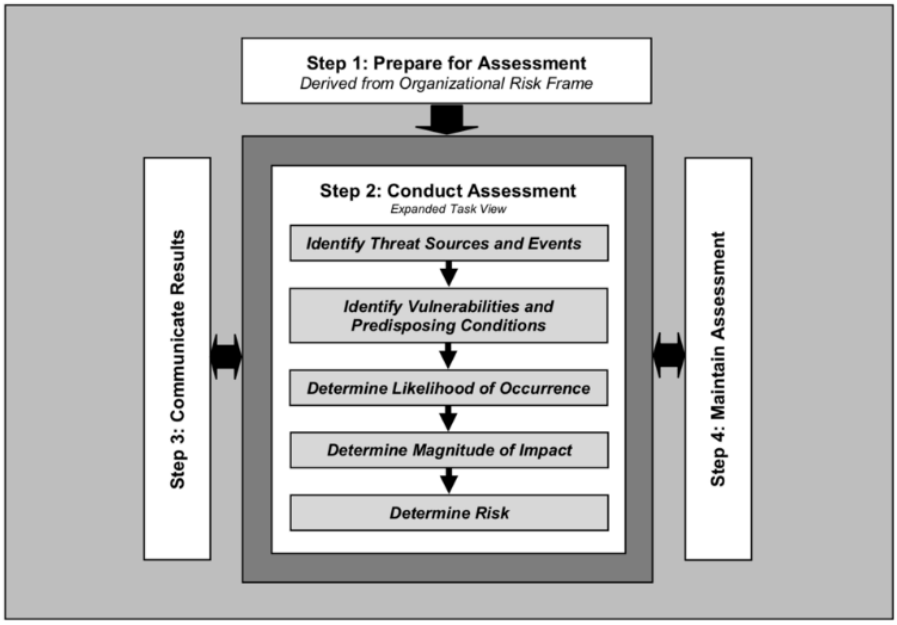

Figure 5: NIST SP-800-30 Risk Assessment Process (NIST, 2012)

Step 1: Prepare for Assessment involves identifying the purpose and the scope of the risk assessment.

Step 2: Conduct Assessment involves the identification of threats, vulnerabilities, likelihood, and impact. There is a range of ways to do so but this depends on the kind of system being assessed and the results of Step 1: Prepare for Assessment.

Step 3: Communicate Results Communicating the results of the risk assessment is one of the most important phases, but often overlooked (CyBOK, 2019). The risk assessment process provides communication and information sharing along the stakeholders. The objective of the communication and information exchange is to make sure that the decision makers in the organization have the right information about the risks needed to make decisions.

NIST (2012) states that: "To be effective, the communication of information security risks and related information needs to be consistent with other forms of risk communication within organizations". The information about risks can be shared via dashboards, briefings, reports and by updating repositories with risk related information and data. Documenting the sources of information about the risk assessment results supports the information sharing, because of the maintainability.

The benefit of risk assessment can be maximized by establishing policies, procedures and implementing mechanisms. This ensures that the appropriate information produced during risk assessments is effectively communicated and shared across all three tiers in the "Risk Management Hierarchy": organization, mission / business processes, and information systems.

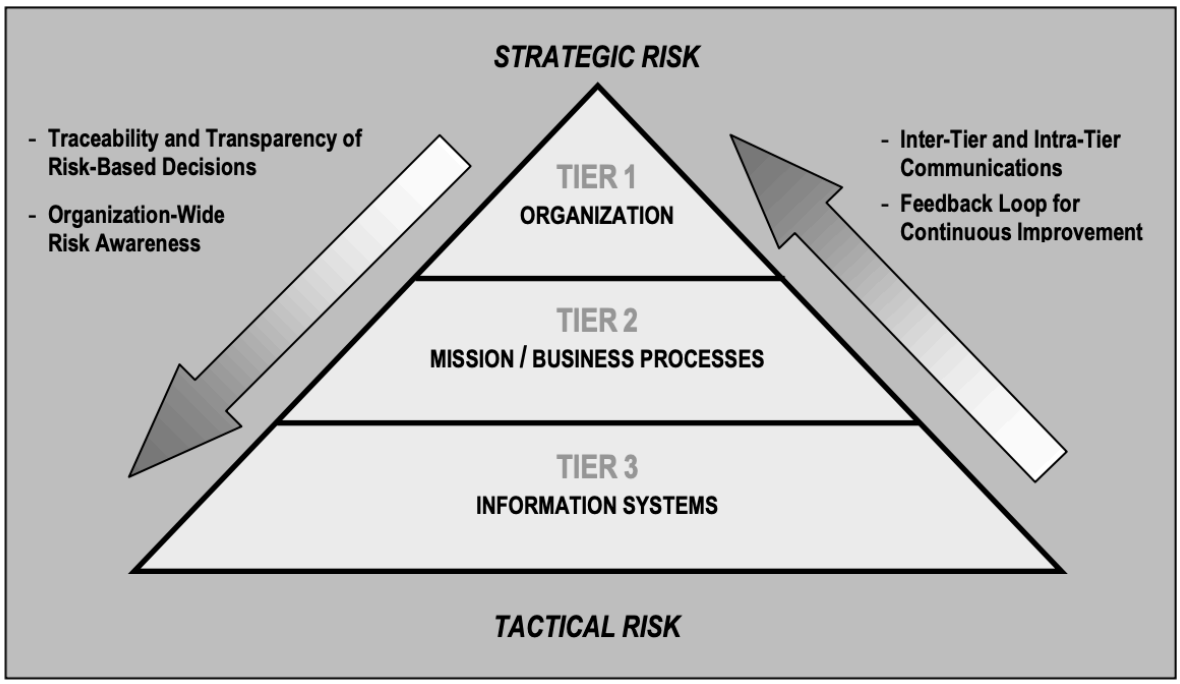

Figure 6: NIST SP-800-30 Risk Management Hierarchy (NIST, 2012)

The risk assessments support different tiers in the risk management hierarchy, illustrated in the figure above, to make risk response decisions. At Tier 3, which is relevant for security operations, risk assessments can affect:

- The design decisions, which include the selection and implementation of security controls and the selection of information technology products for organizational information systems.
- The implementation decisions, whether specific information technology products or product configurations meet security control requirements.
- The operational decisions, which include the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions.

These aspects at Tier 3 are relevant for the interviews and will be discussed in section 2.8.

For Tier 3, the risk assessment results have the following content, which is relevant to identify potential gaps in the information exchange:

- Describe the scope of the risk assessment
- If the risk assessment is relevant for Tier 3, identify the information system(s) name, locations, security categorization, and information system boundary.
- Describe the overall level of risk, for example: very low, low, moderate, high, or very high.
- List the number of risks identified for each level of risk (for example: very low, low, moderate, high, or very high).
- Describe the purpose of the risk assessment, including questions to be answered by the assessment. For example, how the use of a specific information technology would potentially change the risk to organizational missions/business functions if employed in information systems supporting those missions/business functions.
- Describe risk tolerance inputs to the risk assessment.
- Identify and describe the risk model and analytic approach, for example provide a reference or include it as an appendix identifying the different risk factors, value scales, and algorithms for combining values.
- Describe the missions and function if the risk assessment includes organizational missions and business functions,
- If the risk assessment contains information systems, also describe the system(s). For example, the missions and business functions the system is supporting, the information flows to and from the systems, and the dependencies on other systems.
- Finally, summarize risk assessment results. This can be done by using tables or graphs in a way that decision makers can quickly understand the risk, for example the number of threat events, combinations of likelihood and impact.

Step 4: Maintain Assessment during this ongoing phase, it is essential to update continually the risk assessment in the light of changes to the system environment and configuration.

So, the NIST SP-800-30 Risk Assessment Process describes guidelines for conducting risk assessments, including the communication with the organizational decision makers and what information at Tier 3, which is relevant for security operations, should be communicated.

However, it does not describe the information needs of security operations and through what steps this should be shared and translated so that security operations can implement technical controls and react when an actual attack occurs.

ISO/IEC 27005 Process

The ISO/IEC 27005:2018 is an international standard set of guidelines to perform information risk management. This set of guidelines can be used by all types of organizations, for example governments, non-profit organizations, and commercial enterprises, which intent to manage their risks (CyBOK, 2019).

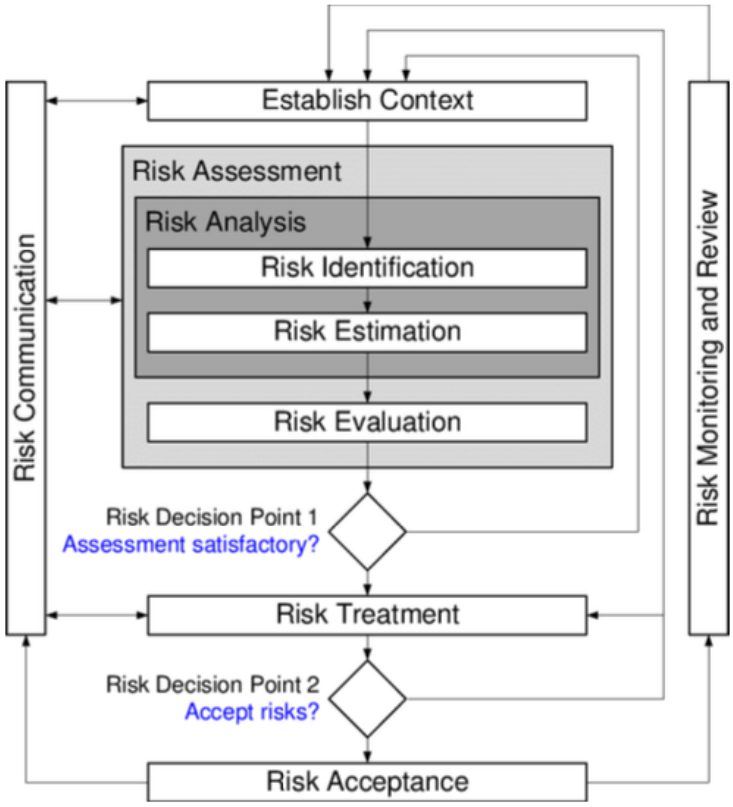

Figure 7: ISO/IEC 27005:2018 Process (S. Rass, 2017)

Description of the different components (Kosub, 2015) / ISO/IEC 27005:

Risk identification: During the risk identification, the organizations context for IT and information security is determined. In addition, the valuable assets and the relevant cyber risks

are identified. Cyber risks need to be identified to manage them. Based on information about the business, valuable firm assets can be identified.

Risk assessment: During the risk assessment, the identified risks are quantified by determining the probability of occurrence and the estimated impact of a risk. This can be done for example by using a risk matrix.

Risk response: During the risk response, adequate risk response measures must be applied based on the results of the risk identification and assessment, for example for risk avoidance (for example avoid use of USB flash drives), for risk mitigation (implement firewalls), for risk transfer (for example cyber insurance), and finally for risk acceptance (for example self-insurance).

Risk control: For risk control, ISO/IEC 27005 demands the monitoring and reviewing of risks. The organization should monitor their risks and control the risk responses regularly and improve these if necessary (for example 24/7 real time monitoring of access to confidential data).

Risk communication: The communication of risk is a dialogue between an organization and its stakeholders. This dialogue is about the different risks that are identified, including their nature, form, likelihood, and significance. In addition, whether these risks are acceptable or not and if these risks should be treated, and what treatment options should be considered. The communication of risk is continual and iterative. It involves sharing and receiving information about the risk management.

The risk information collected from risk management activities is the input for this step, and the output is a continuous understanding of the organization's information security risk management process and results.

Risk communication is critical for sharing and collecting risk data, as well as supporting decision-making, coordinating with other parties, and planning responses to minimize the consequences of potential attacks and incidents. Risk communication plans should be developed for both routine operations and emergency situations. Therefore, risk communication activity should be done on a regular basis.

Risk culture and risk governance: Risk culture and risk governance are required to complete a holistic cyber risk management. The risk culture is important as most of the cyber incidents occur due to actions of people. Therefore, it is necessary to create a risk culture and risk awareness within the organization. In addition, risk governance is important to define a business continuity management plan.

Looking at the ISO/IEC 27005, it does not describe the communication and information exchange with security operations. It describes guidelines on how to perform an information security risk assessment in accordance with ISO27001. This includes "Risk communication", which describes how the communication should be organized with decision makers within the organization, but not specifically with security operations.

STRIDE

Kohnfelder (1999) developed STRIDE, which is a model of threats and can be used to find threats to a system. In this model there are six categories of threats to identify them:

1. Spoofing
2. Tampering
3. Repudiation
4. Information Disclosure
5. Denial of Service
6. Elevation of Privilege

In the STRIDE model, a data flow diagram of the system under consideration is developed and the STRIDE model is applied at each node of this Data Flow Diagram of the system. Then security threats are identified manually. STRIDE does not describe the information exchange and communication of results to organizational decision makers.

Attack trees

Another method for threat modeling is Attack Trees, which is a convenient way to systematically categorize the different ways in which a system can be attacked (Schneier,

1999). This methodology enables security officers to model the IT infrastructure and environment and the associated vulnerabilities. By performing this exercise, the paths than an attack might follow to compromise interesting targets can be identified. The attack graphs quantify the likelihood that an attacker will propagate in a system and the damage (CyBOK, 2019).

This methodology uses a tree structure to represent an attack to a system where the goal is at the root node, and different ways of achieving that goal are the leaf nodes. Each node becomes a sub goal, and children of that node are the ways to achieve that sub goal (Saini et al., 2008).

Attack trees is a methodology used to model threats to a software system, but it does not describe the information exchange and communication of the results to organizational decision makers.

PASTA

PASTA stands for Process for Attack Simulation and Threat Analysis, which is an asset-centric threat modeling approach (Nweke, 2020). PASTA has seven stages:

1. Define objectives
2. Define technical scope
3. Application decomposition
4. Threat analysis
5. Vulnerability & weaknesses analysis
6. Attack modelling
7. Risk & impact analysis

The focus of PASTA is to align technical requirements with business objectives. PASTA analyses the threats and finds possibilities to mitigate them, but more on a strategic level. It identifies the threat, lists the threats, and then assigns them a score. This helps organizations to find suitable countermeasures to be deployed to mitigate security threats.

In line with the earlier described threat modeling methods STRIDE and Attack Trees, PASTA does not contain a prescription of the communication and information exchange with relevant organizational decision makers.

2.4 Using the results of risk assessment and threat modeling

After identifying the threats and risks available, countermeasures have to be reviewed including finding the gaps. Each risk defined during the risk assessment should be reviewed and available counter measures should be mapped to it. The risk that is left is the residual risk. Residual risks should be at an acceptable level, otherwise they still should be reduced by applying more controls.

Countermeasures could be anything, for example adding or modifying firewalls, privileges of user accounts, and shutting down a system (CyBOK, 2019). Information about countermeasures and risk response can also be found in the NIST SP800-39 (NIST, 2012).

However, an impact assessment is required during the deployment of countermeasures. For example, firewall rules or blocked accounts may have a negative effect on an organizations business. This negative effect might even be worse than suffering an attack (CyBOK, 2019).

In the end, not all the risks can be mitigated in an organization. A few must be accepted due to the costs or limitations. However, after implementing the countermeasures, there will still be residual risk left and new threats will emerge. Thus, there is a need for constant monitoring to identify these new evolving threats. Therefore, it is important to keep an eye on the protection controls and indicators.

Leversage and Byres (2008) states that “One of the major requirements for a risk assessment method is to produce simple key security indicators. These key security indicators enable senior management and security experts to take security decisions without getting lost in technical detail”. Key risk indicators (KRIs) can be used to monitor and control risks and to link back to operational risk management activities. These activities and processes include the risk identification, risk assessment, and risk management. Ultimately, a risk indicator can be any parameter that may be used to detect a change in risk exposure over time (Galvanize, 2017).

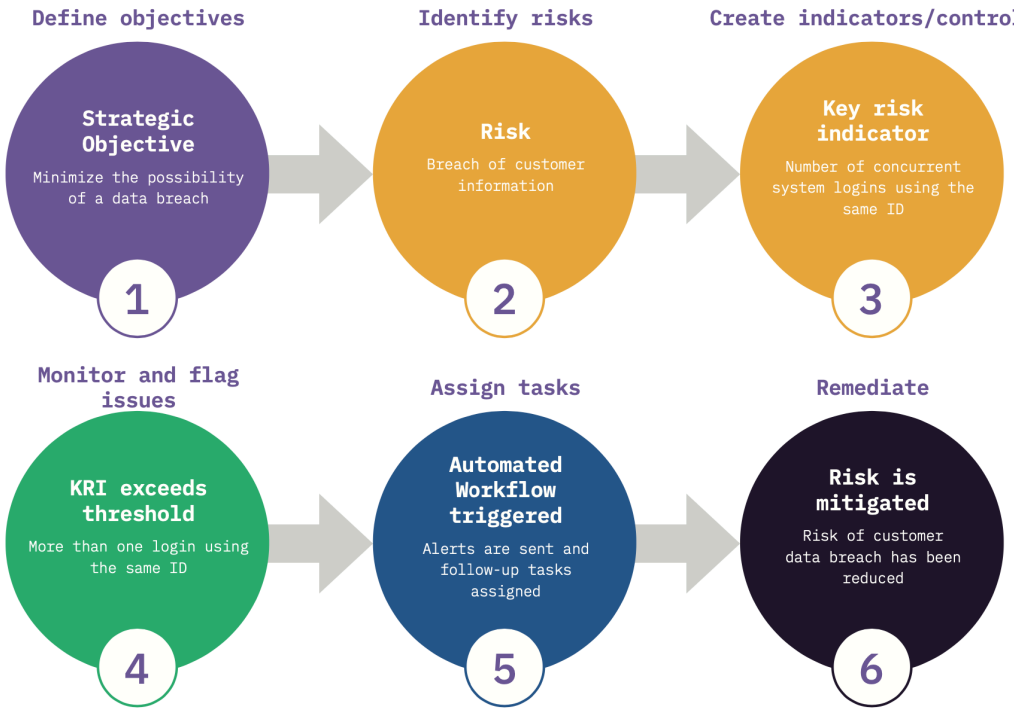

Figure 8: Key Risk Indicator Process (Galvanize, 2017)

It is beneficial to measure KRIs overtime because potential trends can be identified, and contextual information can be provided. Davies, Finlay, McLenaghen, & Wilson (2006) described the need of creating a database of quantitative data that can be used to model the organization's operational risk profile and drive management action in both corrective and preventive terms was stressed.

Thus, these KRIs can be used to monitor and evaluate risks overtime with input from the SOC. KRIs are handed over from the risk analysts to security operations, which report on the activity derived from the monitoring activities. This is relevant for the information exchange between risk assessment and security operations. The results from risk assessment and threat modeling must be communicated to the SOC so that they are able to implement certain security controls and react when an actual attack occurs.

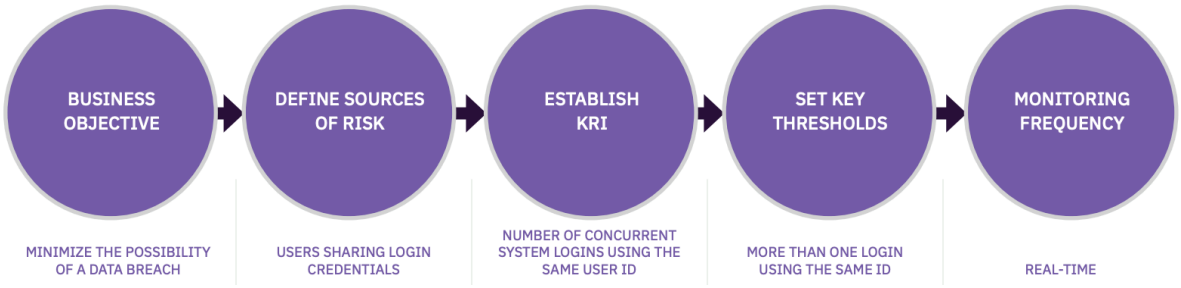

Figure 9: Key Risk Indicator Selection (Galvanize, 2017)

2.5 Security operations

A Security Organization Center (SOC) is a group committed to preventing, detecting, and responding to security incidents. Security Operations Centers are created by companies and governments to defend against computer security attacks. Their responsibility is to monitor, assess, and defend the organizations computing element by using a collection of tools, technologies, and processes. One of the major activities of a SOC is to gather and analyze data, which is incident related. This data is observed in the network of the organization and its end points. To observe these incidents, the SOC gathers, analyzes, and stores massive amounts of data generated by logging methods. Intrusion detection systems, which create logs, are installed on the network, for example to catch potentially hostile actions and to transmit information to SOC analysts. SOCs dedicate a group of people to perform real-time analysis on the alarms, logs, and events that are received on their network. (Kokulu et al., 2019).

For security operations, the current challenges and trends described by (Deloitte, 2020) are:

- **Expanding attack surface**

Businesses are quickly altering their business models and corresponding technological infrastructures to compete with one another. To satisfy more flexible business demands, enterprise data that was formerly kept under lock and key is now being shared across different business divisions, partners, and external suppliers. As technology continues to empower enterprises, the attack surface of organizations will increase further.

- **Security talent shortage**

One the most critical challenges of cybersecurity today is the shortfall of talented and skilled people. The number of people having the vision, experience and skills is not growing fast enough.

- **Too many alerts from too many tools**

More and more IT assets need to be secured, which results in more security tools, more alerts, and more threats. Security operations in the future will rely on humans powered by automation for making better and quicker decisions regarding observed security signals.

There are different roles and responsibilities in the SOC. Tier 1 is the first group of system analysts, who have the responsibility to monitor real-time and to configure system tools. If the incident is out of scope or their skill set is not enough to investigate that incident, they escalate it to Tier 2. Tier 2 then perform an in-depth analysis of the incident and take actions such as blocking an activity, deactivating an account, or escalating the case to a higher tier.

Tier 3 analysts are comparable to Tier 2 analysts, but Tier 3 is more experienced with high-level incidents, vulnerability assessments, penetration testing, alerts, industry news, threat intelligence, and security data. Tier 3 is constantly looking for threats that have infiltrated the network, including unknown vulnerabilities and security issues.

For security monitoring, the threats are a core driver, including other aspects of the organizational environment:

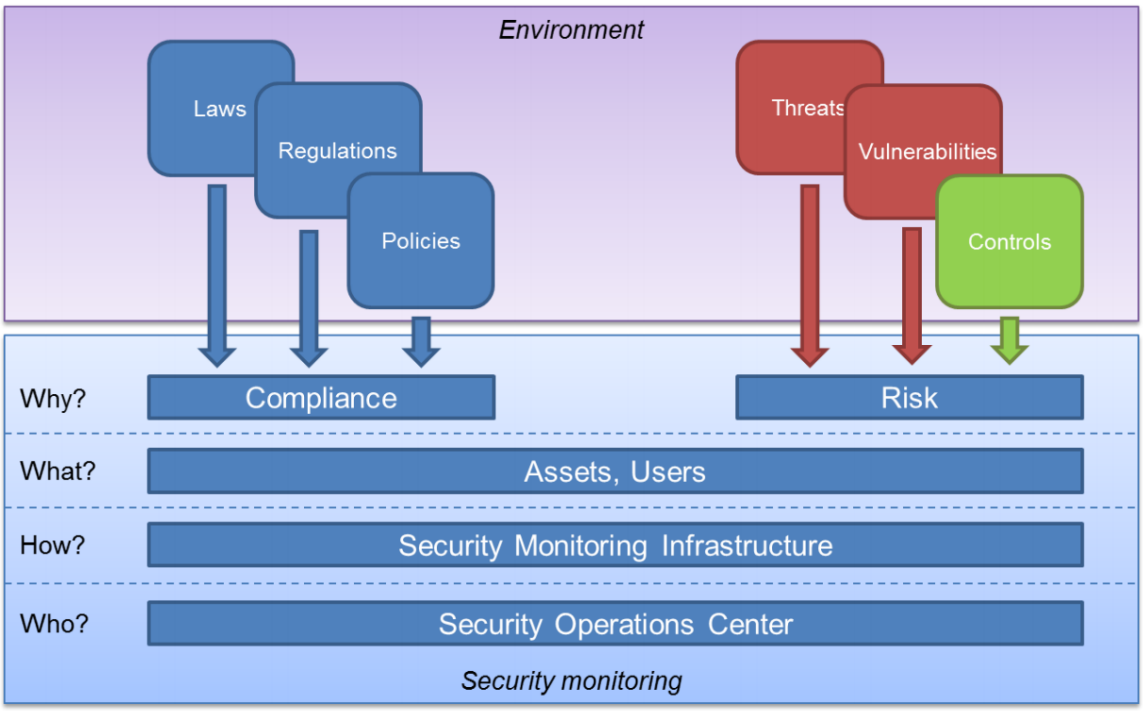

Figure 10: Security monitoring environment (MaGMA, 2017)

A security monitoring system is used to support the security monitoring process. A SIEM (Security Information and Event Management) system is an important component of security monitoring (MaGMa, 2017). Figure 11 shows an example of a security monitoring infrastructure.

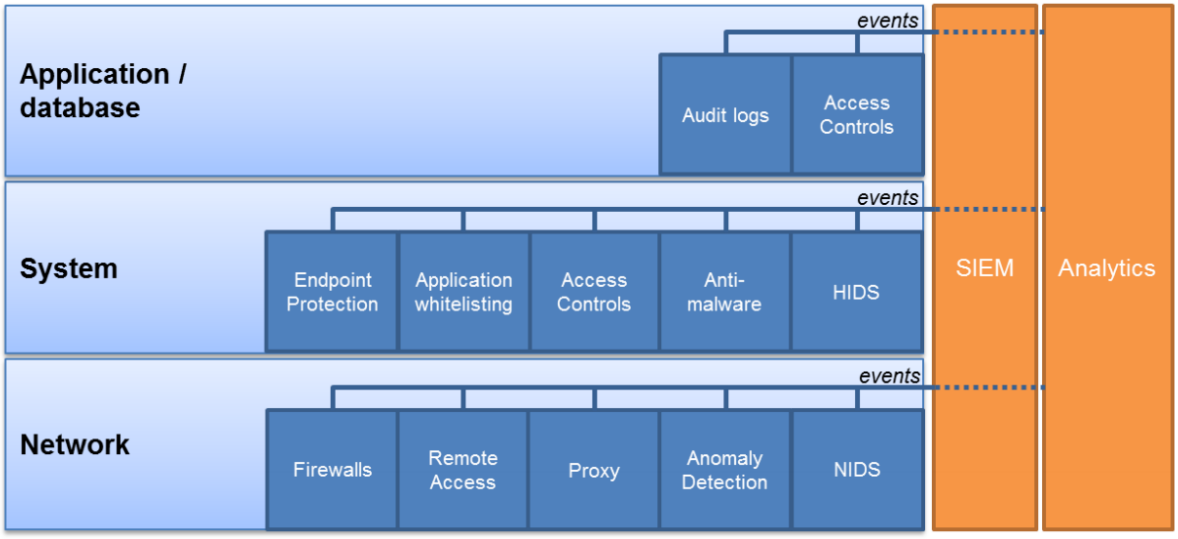

Figure 11: Example security monitoring infrastructure (MaGMa, 2017)

The SIEM tooling aggregates data from multiple systems and analyzes those data to catch abnormal behavior or potential cyberattacks. To do this, SIEM tools make use of use-cases, which help and support security analysts to provide a structured approach to security monitoring. Use-cases convert business threats from risk assessment and threat modeling into technical SIEM rules, which then detect possible attacks or threats and send alerts to the analysts. This means that use-cases can determine whether an attack will be detected or not and at what stage a threat will be detected (MaGMa, 2017).

A use-case can be a combination of several technical rules within the SIEM tool or a combination of actions from multiple rules. It converts business threats from risk assessment and threat modeling into SIEM technical rules, which then detect possible threats and send alerts to the SOC. It also suggests taking actions in response to current or previous activities that could be part of a current or future attack. Use-cases can determine whether an attack within the network will be detected or missed, and at what stage incoming threats can be detected (IBM, 2020). Another part of the use-cases are the follow-up actions (incident response) that are tied to the business drivers. These can show security monitoring is reducing risk for the organization. To implement these use-cases different information is needed regarding different use-case layers (MaGMa, 2017):

Business layer

The first layer of the use-case is the business layer, which addresses the elements that are relevant to ensure that the use-case supports the business and vice-versa:

- The purpose of the use-case and its relevance for the business should be made clear.
- The drivers for the use-case are usually risk reduction, reputational damage, or compliance drivers.
- The main stakeholders that are involved for this use-case.

Tactical layer

The tactical layer of the use-case is used to align the use-case with the threat management processes:

- Threats that are addressed by the use-case.
- Threat actors that are relevant for the use-case.

- The actions that need to be taken when security monitoring alerts are fired relating to the use-case. It is important to determine the appropriate response before implementing the use-case because significant added value from the SOC comes from incident response (incident response).
- For analysts, it is helpful to have some guidance on analysis alerts generated by security monitoring rules (security analysis).

Implementational layer

Finally, the implementational layer of the use-case addresses the organizational aspects of the use-case in the security monitoring architecture:

- The rules, which detect and trigger alerts based on targeted events
- The logic, which defines how events or rules will be considered
- The action, which determines what action is required if logic or conditions are met
- The logfiles, what log sources can provide input into this use-case

A use-case goes through several stages to complete its cycle, from planning to deployment (IBM, 2020):

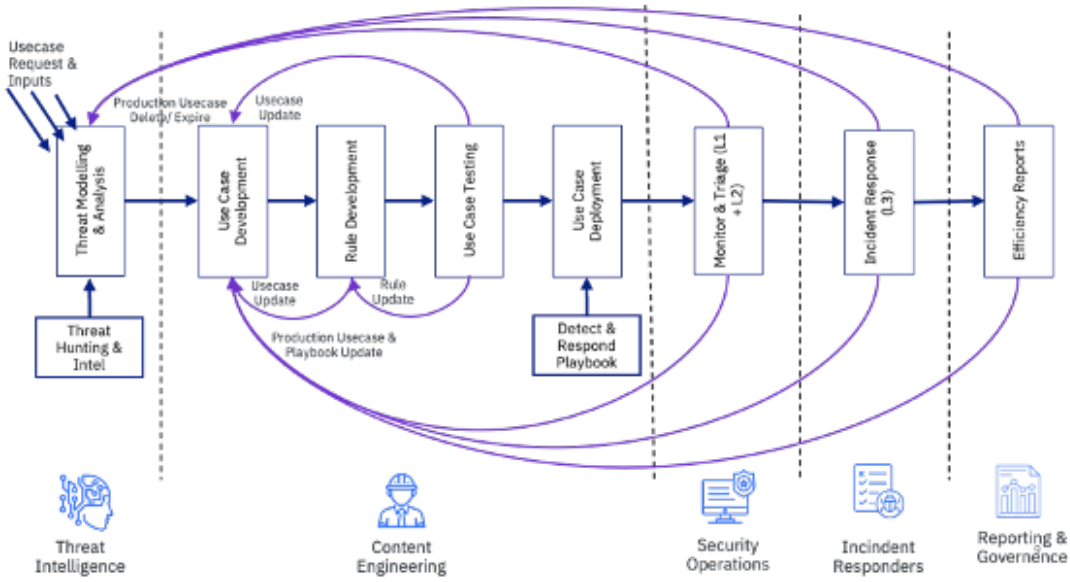

Figure 12: The Lifecycle of SIEM Use-cases (IBM, 2020)

Define/Review Requirements: During the first stage, business threats and risks are defined before setting up SIEM use-cases (risk assessment / threat modeling).

Identify Data Source: The next step is to identify where this information can be found.

On-/Off-board Data Source: After identifying the data sources, they are integrated into the SIEM. This integration could require some configuration at the source depending on the SIEM in place.

Design/Review Logic: During this step it is observed what needs to be detected and attacked (the event fields). An important factor while building this logic/rule is identifying the correct event field to perform correlation or aggregation.

Define Baseline: Next, to aggregate similar events inside the use-case, thresholds and baselines must be specified.

Testing and Tuning: After defining the baseline, the defined logic and baseline in the use-case need to be tested. Based on the testing results, tuning is required to ensure noise is reduced.

Optimize Based on Outcome: Based on the testing, the baselines are optimized to detect an attack.

Monitoring Performance: Finally, a use-case is deployed in production and monitored to analyze its performance and alerts, generated to keep a check on false positives and overall health.

Thus, the SIEM and use-cases are relevant for the communication and information exchange. Security operations need to implement use-cases within the SIEM to monitor the risks that are identified during the risk assessment. Follow-up actions (incident response) are described in use-cases, which are linked to the business drivers to demonstrate how security monitoring reduces risks in the organizations. It is important that security operations have the right information to their disposal regarding the business layer (purpose and drivers), the tactical layer (threats, actor, security incidents response, and security analysis), and the implementation layer (log sources, rules, logic, and action) to make the translation from a risk / threat to the

technical implementation of a use-case. This is the information that security operations need to implement a monitoring solution and to be able to respond to an actual attack. It is relevant for this research to examine if risk assessment provides this information or if information is missing.

2.6 Conclusion

During the literature review we looked at the concepts of risk assessment, threat modeling and security operations to learn what kind of research already exists about the communication and information exchange between risk assessment and security operations. This includes the relationship between the concepts and what methods / frameworks are available, including their characteristics in order to answer the following research question:

"How is the information exchange organized according to the methods and best practices in security risk management, threat modeling and security operations?"

We analyzed different frameworks and method regarding the communication of risk assessment / threat modeling results. NIST SP-800-30 Risk Assessment Process provides guidance for conducting risk assessments, including the communication of the risk assessment result (including document formats). It describes what information is relevant for Tier 3 and how it could be communicated, which is relevant for security operations. Information could be shared via dashboards, reports, and briefings, and by adding supporting evidence of risk assessment results to risk-related data repositories. Documenting the sources of information, analytical procedures, and intermediate results also supports the information exchange, making risk assessments easier to maintain (NIST, 2012). The information that is shared contains primarily the identified risks, design decisions, implementational decisions, and operation decisions.

Regarding security operations, SIEMs and use-cases are relevant for the communication and information exchange. Security operations need to implement use-cases within the SIEM to be able to detect and react to attacks. To implement these use-cases, information about the business layer, the tactical layer, and the implementation layer are needed. It is relevant for this research to examine if risk assessment provides this information or if information lacks.

With input from the SOC, KRIs (Key Risk Indicators) can be used to monitor and evaluate risks overtime. KRIs are handed over from the risk analysts to security operations which report about the activity derived from the monitoring activities.

So, based on the literature review, in order to be able to translate the risks and threats into security controls, communication and information exchange between risk assessment and security operations is necessary. There is an information exchange with organizational decision makers and security operations to translate the risks and threats into a monitoring solution. However, when we compare the results of the risk assessment with the information needs from security operations, a gap can be observed. The results of the risk assessment cover the business layer, but they do not include information about the technical layer and the implementation layer in terms of technical information about threat management and the security monitoring architecture.

Besides that, it is not clear what the process of risk assessment to monitoring and detection looks like. It is neither clear what information is exchanged in practice. These observed gaps in the literature will form the input for the survey questions that aim to describe the gap between risk assessment / threat modeling and security operations. Also, the NIST described that for Tier 3, the organization decision makers can make decisions based on the risk assessment in terms of design, implementation, and operations. For this research and these survey questions we will cover this part. We aim to examine how risks and threats are evaluated overtime, and to see if the monitoring is effective and reduces risks for the organization. To find out how this is done in practice, the evaluation of the threats and risks is incorporated within the interview questions (see Appendix A: Interview questions risk assessment / security operations.)

Method

This chapter begins by making clear what is meant by exploratory and qualitative research and why we adopt such methodology. Further down the section, it argues about the theory building, together with the data collection and different techniques.

3.1 Research strategy

The objective is to research the information exchange and communication channels between the risk assessment and threat modeling and security operations to see what is missing (gap) and how it could be improved. By doing so, a potential increase in effectivity, efficiency (less resources) and security level could be achieved.

RQ: "What is the gap between risk assessment and security operations and how could this be improved?"

General

The aim of the research and objectives are primarily exploratory in nature. We use qualitative data collection methods and analysis methods (for example qualitative content analysis). In this research we try to understand and describe what the gap is. In addition, we attempt to find possible improvements for the information exchange and communication channels. To do this, we use exploratory research. The aim of exploratory research is to find answers to the questions of "what"'.

To get an insight in the information exchange practices between risk assessment / threat modeling and security operations, it is important to interact with the experts working within the field, and to gain information and knowledge in the form of experiences, beliefs, and attitudes. This insight cannot be achieved easily through conducting surveys and interviews using closed questions. Therefore, we use qualitative research for this research.

Qualitative research is an examination into facts or principles aimed to describe and clarify human experience as it appears in people's lives (Polinghorne, 2005). Qualitative methods are used by researchers to gather data that serve as evidence for their distilled descriptions. This qualitative data is gathered primarily in the form of written or spoken language rather numbers. Data sources that could be used for gathering qualitative data are interviews with participants,

observations, documents, and artifacts. The qualitative data is translated into written text for analytical use.

We conduct a series of interviews with open-ended questions to gather qualitative data and further analyze to find broad patterns in their responses using the grounded theory.

3.2 Data collection techniques and procedures

In this section we describe the data collection techniques and procedures that we use to answer the research questions.

- **Sample**

In order to investigate the gap, the interviewees are divided into two groups: Risk assessment / threat modeling (RA) and security operations (SO). We have chosen to do so to integrate both viewpoints. An interviewee is qualified based on role, experience, educational and kind of organization. Examples of the different roles are risk modelers, risk managers, security designers, cybersecurity consultants, security operation managers and security analysts. Based on the role and previous experiences of the interviewee, a certain role is determined. The goal is to have a distribution of 50/50 for each role and to interview practitioners from different companies to improve the generalizability of the findings. This generalizability is due to different standpoints, views, and expressions. The kind of organization is a firm that delivers cybersecurity services to their clients in the form of risk assessment and monitoring & detection. Four companies, which are all based in the Netherlands, participate in total.

- **Semi structured interviews with open-ended questions**

By using semi structured interviews, a researcher has the flexibility to improve them, or change direction as new themes emerge and the research progresses. This is the case despite a pre-identified guide with open-ended questions (Jamshed, 2014). By using open-ended questions, experts can express opinions that may be unusual, or simply ones that we did not think about. This would not be possible using closed questions.

We record and transcribe the interviews and afterwards we send the transcripts to the interviewees for conformation. At the start of the interview, we disclose the interviewees their

rights and privileges regarding the GDPR (purpose, what kind of information, how long the recording will be maintained). We use one-on-one interviews to capture the perspective of only the interviewee and minimize the chance that the interviewee's perspective will be altered because of the input from others. For the interviews we use conferencing software because of government restrictions due to the COVID-19 pandemic. For analyzing purposes, the interviews are recorded. This way they can be transcribed.

- **Grounded theory like approach for qualitative data analysis**

(Glaser and Strauss, 1967) first mentioned theoretical sampling and described a process of generating theory from data, which includes collecting the data and then coding and analyzing the data. One of the key activities to implement the Grounded theory approach for theory building is coding. Coding can be seen as the process of labeling and organizing qualitative data to identify different concepts and the relationship between them. We use a Grounded Theory like approach, where we conduct different steps to build a theory by interpreting and understanding the broad patterns visible in the data collected through interviews at the different companies, in order to describe the gap and possible improvements. To do so, we conduct the following steps that are involved in the Grounded Theory (Straus and Corbin, 1990):

Open coding

Open coding involves line-by-line coding where we assign codes to the main ideas and expressions within the transcriptions. Also, we identify codes with similar properties, which we group together under the heading of a concept to give it a meaningful form. By doing this, we can break down the data into conceptual components and we can start to theorize or reflect on what we are reading. We constantly compare the data from each participant for similarities.

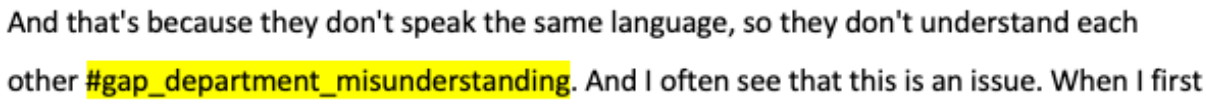

Figure 13: Example open coding

Axial Coding

At this stage, we identify relationships and connections between the different concepts and identified categories. We compare the categories that are identified and try to find the relationships in the data.

Gap
Communication
Information exchange
Resources

Figure 14: Example axis coding

Selective Coding

During the selective coding, we identify the core categories and methodically relate them to other categories. We identify theories by integrating the different categories and refining the relationships further.

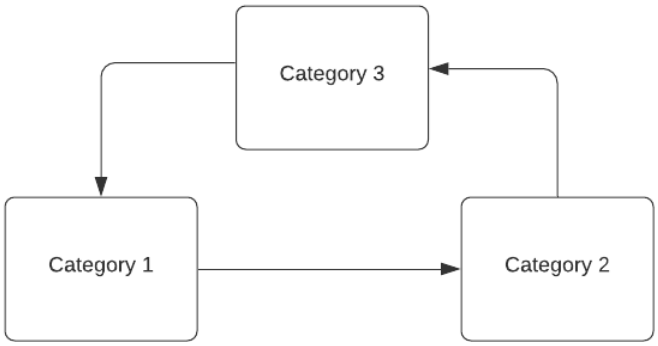

Figure 15: Example selective coding

The resulting process will look as shown in the figure below:

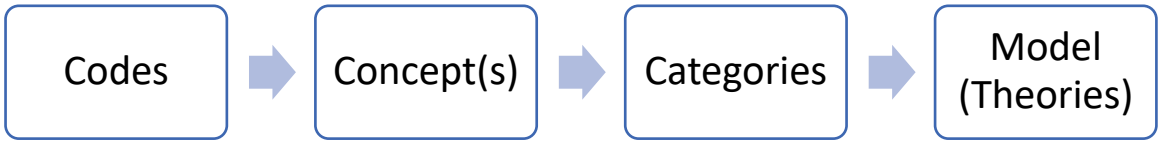

Figure 16: Process grounded theory

Results

This section presents the outcome from the data collected and analyzed through the interviews and contextualized further to arrive at findings. The first section presents the statistics of the interviews and participants and the collected data. After the statistics and data, the results are described based on the gaps identified during the literature review and interviews. Before the gap description the general process is described to understand the gaps and improvements. To illustrate the results, quotations from the interviews are included. Quotations that were originally in Dutch have been translated to English.

4.1 Statistics interviews

For this research, a total of eleven experts were interviewed. This includes five experts performing risk assessments / risk analysis and six security operations experts in the role of manager, consultant, or team lead. Ten of the eleven interviews were conducted through Teams because of the COVID 19 situation, and one interview was conducted through face-to-face contact. Ten experts were interviewed in Dutch and one expert in English. Both the Dutch and English interviews were coded using English codes. The Dutch transcripts have not been translated due to time restrictions and to prevent bias occurring in the translation of words. The questionnaire can be found in de Appendix A: Interview questions.

General statistics

	RA (n=5)	**SO (n=6)**	**Total (n=11)**
Average duration (min)	40	34	37
Range (min)	28-59	31-67	28-67

Table 3: General statistics interviews

- **Overview experts**

Interview	Risk assessment / security operations	Role	Experience
1	RA	Security Operations Manager SOC	4 years
2	RA	Manager Security Advisory	6 years
3	SO	Security Operations Manager SOC	5 years
4	SO	Team Lead Security Operations	5 years
5	RA	Program Manager Cyber Security	5 years
6	RA	Business Security Consultant	6 years
7	SO	Security Operations Manager	5 years
8	SO	Manager Blue Team	4 years
9	RA	Director Business Security	11 years
10	SO	SecOps Tech Lead SOC	13 years
11	SO	Manager SOC operations	3 years

Table 4: Overview experts

- **Statistics experts**

		RA (n=5)	SO (n=6)	Total (n=11)
Roles	Manager	2 (40%)	3 (40%)	5 (45%)
	Consultant	1 (20%)	1 (20%)	2 (18%)
	Officer	0 (0%)	0 (0%)	0 (0%)
	Director	2 (20%)	0 (0%)	2 (18%)
	CTO	0 (0%)	0 (20%)	0 (0%)
	Team lead	0 (0%)	2 (40%)	2 (18%)
Years active	Median	6	5	5
	Minimum	4	3	3
	Maximum	11	13	13

Table 5: Statistics experts

4.3 Codes and categories

In this section the results of the coding process will be described from the application of the Ground Theory to the transcripts of the interviews, including a reflection on the coding process.

The intention was to perform interviewing, transcribing, and coding iteratively to determine when theoretical saturation is reached. Strauss & Corbin (1998) describe theoretical saturation as "The point in category development at which no new properties, dimensions, or relationships emerge during analysis". Therefore, transcribing and coding started after the first interview had been administered. Because coding took more time than anticipated, the process has not been done fully iteratively.

To ensure that the data of the codebook are reliable, partial double coding has been performed. This has been done by coding part of qualitative data set to an external individual to compare the different codes using the same steps. Some disagreements occurred about the different application of codes and the place where the codes are placed in the sentences. But in general, the codes from the external individual matched the codes that we came up with.

By the open coding a total of 607 codes spread along the eleven interviews that were conducted with the experts:

Interview	Number of codes
1	59
2	93
3	59
4	31
5	63
6	58
7	57
8	53
9	58
10	47
11	29

Table 6: Number of codes interviews

The following table captures codes, which were mentioned more than four times across all interviews. Most of the codes are concerned with risk analysis, security operations, use-cases, monitoring, and evaluating. Other codes of interest are assessments, onboarding, threats, and frameworks. Remaining codes are concerned with onboarding, communication, improvements, information, threat intelligence, and security management.

#	Values	Number (codes)
1	Analysis	57
2	Security operations	52
3	Use-cases	46
4	Monitoring	36
5	Evaluation	32
6	Assessment	24
7	Onboarding	22
8	Threats	20
9	Framework	20
10	Gaps	19
11	Report	19
12	Method	17
13	Threat intelligence	15
14	Incident	15
15	Improvements	14
16	Collaboration	14
17	Mapping	13
18	SIEM	12
19	Scenario	11
20	Measure	11
21	Translation	10
22	Results	9
23	Context	9
24	Scope	8
25	Output	7
26	MITRE	7
27	Log-files	7
28	Communication	6
29	Insight	6
30	Joint exercise	6
31	Detection	4
32	Governance	4
33	Technique	4
34	Reduction	4

35	Thresholds	4
36	Behavior	4
37	Knowledge	4
38	Language	4
39	Quality	4
40	Compliance	4
41	Alert	4

Table 7: Number of codes

In the following section, the research questions that were relevant for the interviews are mapped with the interview questions, including the concepts that were derived from the interviews. A concept contains codes which relate to each other. Analysis of the initial codes led to insights in patterns and recurring themes. All interview questions can be found in Appendix A: Interview questions risk assessment security operations. To understand the context of the gaps and improvements, the process is described first in terms of the concepts. Afterwards, the concepts that are identified for the gaps and improvements are specified per interview question.

4.3.1 Process

To describe the current process, the following categories, sub-categories, and number of concepts were identified through axial coding:

Category	**Sub-category**	**Number of concepts**
Risk analysis	Risk management	27
Risk analysis	Risk assessment	18
Risk analysis	Risk definition	18
Risk analysis	Threats	15
Total		**78**

Table 8: Distribution of concepts risk analysis

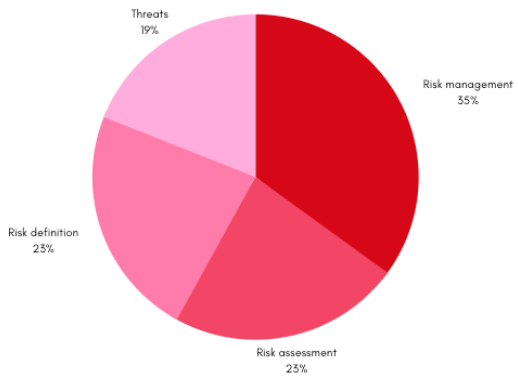

Figure 17: Distribution concepts risk analysis

Category	Sub-category	Number of concepts
Security operations	Detection	24
Security operations	Monitoring	20
Security operations	Use-case implementation	20
Security operations	Evaluation / reporting	8
Total		**72**

Table 9: Distribution of concepts security operations

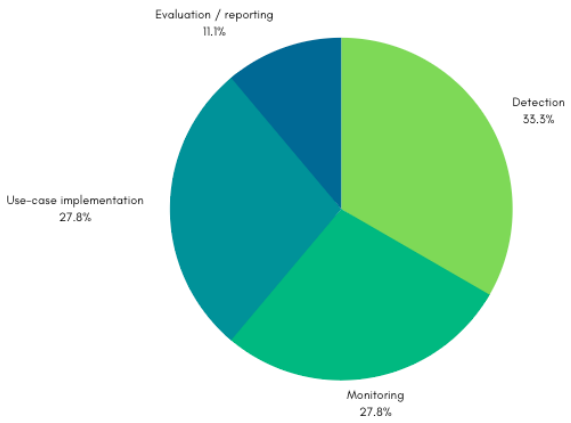

Figure 18: Distribution concepts security operations

Category	Sub-category	Number of concepts
Translation	Onboarding	14
Translation	Technical translation	13
Translation	Communication	4
Total		**31**

Table 10: Distribution of concepts translation

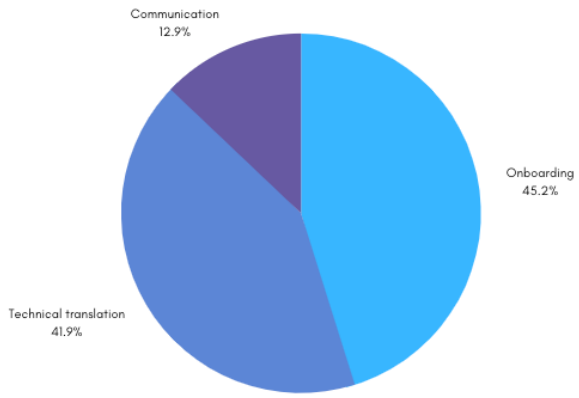

Figure 19: Distribution concepts translation

Category	Sub-category	Number of concepts
Information exchange	Gaps	13
Information exchange	Improvements	8
Total		**21**

Table 11: Distribution of concepts information exchange

See Appendix B for all identified concepts per (sub)category.

4.3.2 Gap identification communication and information exchange

SQ2: "What is missing in the information exchange between risk assessment / threat modeling and security operations?"

To identify the different gaps in the information exchange, the following questions were asked during the interviews for risk assessment and security operations. This resulted in the following concepts:

Concepts per interview questions Risk Assessment (RA)

Question 1: What are the results / kind of information that you get after performing these mapping exercises (RA / TM)? In terms of identified and the format of this information. o What actions are taken after the mapping exercises? To which persons do you communicate these findings? And how?	
Concepts question 1	
Risk	Landscape
Threats	Presentation
Roadmap	Technical deep-dive
Evaluation	Session
Appetite	Risk report
Summary	SOC
Current measures	Scenarios
Question 2: How does the process of longer-term monitoring of the identified threats and risks look like? To see if the measures are taken and if the threats are in control. o Do you use Key Risk Indicators to monitor this? If not, how do you monitor this? o And who is responsible?	
Concepts question 2	
Reporting	Monitoring cycles
Security Officer	Input SOC
Difficulty	Incidents
Variants	Interval

Question 3: Are there any activities that ensure communication of the risks to the SOC team in order to monitor this? o If yes, what information is shared with the SOC? o In what form and in what kind is the information being shared? (Meetings / Key Risk Indicators e.g.) o Which person receives the information? o If no, what is the reason and how could it be done?	
Concepts question 3	
Meetings	Use-case
Risk identification	Security Operations Manager
SOC	Context information
Risk report	Technical discussion
Organizational structure	
Question 4: Can you describe the relationship of risk assessment with security operations / SOC?	
Concepts question 4	
Risk analysis input	Governance
Evaluation monitoring	SOC Reporting
Collaboration	Method difference
Question 5: Do you use inputs from SOC for the risk assessment and threat modeling? o In terms of data about likelihood or specific events for example? o Anything else?	
Concepts question 5	
Risk evaluation	Trends
SOC input	Threats
Use-case output	Threat response
Incidents	Threat intelligence

Table 12: Mapping interviews questions and concepts gaps for risk assessment

Concepts per interview question Security Operations (SO)

Question 1: How do you receive information about risks & threats / controls / use-cases from risk assessment and threat modeling that have to be implemented for a client? How is information being exchanged?	
Concepts question 1	
Information completeness	Technical deep-dive
Information check	Risk report
Meeting	Translation
Projects	Hand-over
Question 2: How do you integrate the information from the risk management and threat modeling team into your processes? o E.g., are you tasked to implement recommended controls? o Do you have a way to consume the identified threat scenarios and monitor for those? o Do you receive any Key Risk Indicators for monitoring?	
Concepts question 2	
Use-cases	Implementation plan
Translation	Follow-up
SIEM	Security engineer
Playbooks	Work instructions
Documentation	Tooling
Question 3: What kind of information do you need from risk management and threat modeling to improve the security operations and to be able to better respond to actual attacks? o In what kind of format? o Do risk assessment and threat modeling provide this information to implement reactive and corrective controls when an attack occurs? Is there anything missing?	
Concepts question 3	
Context information	System-information

Log-files	Thresholds
(Ab)normal behavior	Technical
Question 4: Do you provide any data/information to the risk management and threat modeling team or participate in their activities? o (e.g., supply likelihood estimates, consult them on observed threats or recent threats from the threat intelligence feeds)?	
Concepts question 4	
SOC Reporting	Risk evaluation
Insights	Security Officer
Monitoring efficiency	

Table 13: Mapping interviews questions and concepts gaps for security operations

Concepts problems and gaps Risk Assessment (RA) & Security Operations (SO)

Are you encountering problems / gaps in the process, communication between risk assessment and security operations? o If yes, can you explain?	
Concepts	
Misunderstanding	Collaboration
Language difference	Resources
Use-case lifecycle	Methods used
Translation difficulty	Governance
Reporting	Consistency
Effectivity insight	Knowledge gap

Table 14: Mapping interviews question and concepts gaps for risk assessment and security operations

By analyzing these concepts, we have identified relevant data for answering the research questions regarding the gaps and improvements. The different concepts for the gaps are categorized through axial coding:

Gaps identified between risk assessment / threat modeling and security operations

	1	2	3	4	5	6	7	8	9	10	11	Total	% of the interviewees
Translation of risks / threats to a technical solution	X		X				X		X	X		**6**	**54%**
Business / technical orientation (knowledge gap)	X		X	X			X		X	X		**5**	**45%**
Evaluation / reporting		X				X			X		X	**4**	**36%**
Use-case lifecycle management							X	X				**2**	**18%**

Table 15: Distribution identified gaps

The gaps in the communication and information exchange are described later in more detail because of their relevancy to the research questions (section 4.5).

4.3.3 Improvements

SQ3: "What process or guidelines can be implemented to improve the information exchange between risk assessment / threat modeling and security operations?

Question (RA & SO)

Question: Are you encountering problems / gaps in the process, communication between risk assessment and security operations? o If yes, can you explain? o **What could be possible improvements?**	
Concepts	
Language overlap	Joint exercises

Middle agreement	Difficulties to bridge the gap
Common understanding	Method overlap
Identify information needs	Baseline

Table 16: Mapping interview question and concepts for the improvements

Like the concepts identified for the gaps, the different concepts for the improvements are categorized through the axial coding:

Identified improvements between risk assessment / threat modeling and security operations

Interviewee-Improvement	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**Total**	**% of the interviewees**
Joint exercises / common understanding (language overlap)	X		X	X			X		X	X		**6**	**54%**
Establish baseline							X		X			**2**	**18%**
Identify information needs			X							X		**2**	**18%**

Table 17: Distribution codes identified improvements

Again, the improvements are described later in more detail because of their relevancy to the research questions (section 4.6).

After the axial coding, selective coding integrates the relationships found in the second step and refines them further:

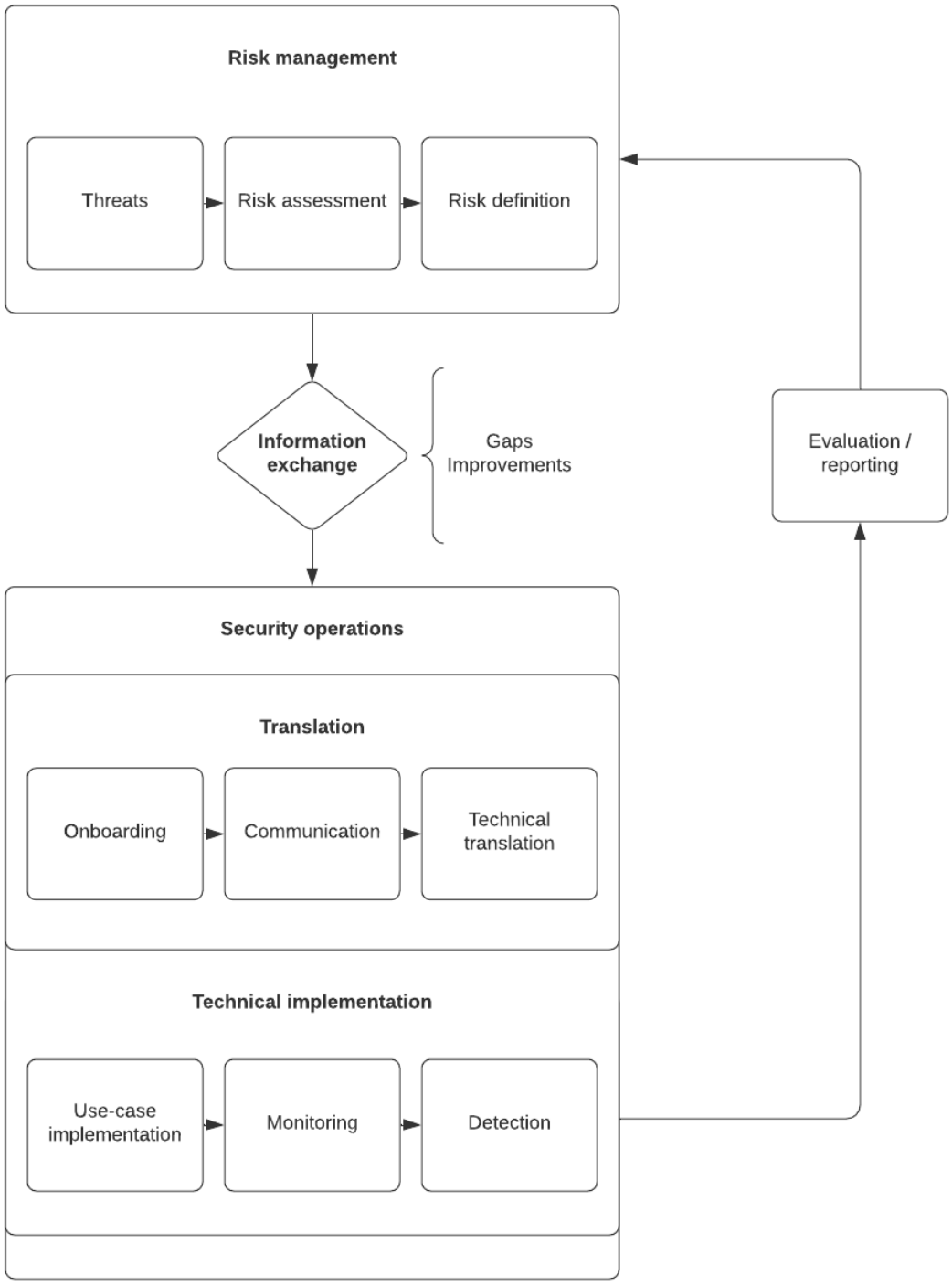

Figure 20: Current process based on grounded theory

The process, gaps, and improvements are described in the following sections according to the results of the qualitative dataset analysis.

4.4 General

To understand the different gaps, we first describe the way a risk assessment is performed by the risk managers / consultants and the results of this exercise. This can then be compared to the information needs of security operations. Also, during the literature review it was unclear what the process from a risk assessment to a monitoring solution looks like. We will describe this according to the results of the interviews:

Risk assessment

To implement monitoring and detection for a client, an organization needs to have an indication of the specific risks in relation to information security. Most experts stated that the methods and standards that are used for conducting risk assessment and threat modeling depend on the kind of customer and situation. Governments and banks use different frameworks in comparison to other private sector companies. Organizations tend to develop their own methods based on the more common frameworks.

First, context information about the organization is needed. This entails identifying the key assets and establishing what the processes look like. Based on this information, a session with the most important stakeholders in the organization is done, for example management (the director of IT, HR, Finance, Operations). Prior to this session, the risk appetite of the organization is determined.

After the risk appetite is determined, the risks are collected broadly within the organization. When the context is determined, the risk analysis is performed: What is most important at a strategic level? What are the strategy and objectives of the organization? What risks are involved? And how are these risks classified? The classification is done based on the financial or reputational damage determining the probability and impact.

Based on the identified risks: What is the current status of any measures that have already been taken at this moment, and which may already be lowering these risks. As a result, net risks come out. Based on the net risks, a treatment plan is written on how to ensure that the risks are managed to an acceptable level. This includes what measures must be taken.

However, one of the experts from security operations states that: *"Not every customer has performed such a risk analysis by us. So, to ensure that the monitoring we offer to the customer is nevertheless risk-based, we will examine with the customer at a technical level to see what risks we can cover."* [Interview 3 – Security Operations Manager SOC]

In some cases, an organization decides to have a monitoring solution implemented by a security firm, without having a broad risk analysis beforehand. In that situation, an organization chooses to have a monitoring solution only. Security operations themselves then examine at a technical level what risks can be covered to ensure that the monitoring is risk-based. There is a difference in the way risk assessment is done by the different departments (risk department and security operations). When the risk analysis is performed by the actual risk department / risk managers / business security consultants, the scope is broader in comparison to the one of security operations, which is more focused on the technical level.

One expert states about the limited scope: *"The advantage of the limited scope is that it goes fast, probably. The disadvantage of this is that you do get a bit of tunnel vision, I think, because you then start implementing things that are easier to implement."* [Interview 7 – Security Operations Manager]

The same expert stated:

"I understand that, because to be very honest, the scope is one of the most difficult things in the preliminary phase. If you do it too broadly, then you as a SOC can't do much about it, because then you think: you ask the whole world, that is not possible. If you make it too narrow, you may miss things. [Interview 7 – Security Operations Manager]

The question is how a more strategic business risk analysis can be done here, so that security operations can monitor the right use-cases, which contributes to the business strategy and objectives.

Risk assessment results

After conducting the risk assessment, the different risks and threats applicable for an organization are identified. Then, a treatment plan will be presented to the organizational decision makers.

This is a strategic roadmap, including the risks / threats and recommendations containing:

- Risk appetite
- Approach
- Risks
- Assessment of the risks (probability / impact)
- Current measures
- Recommendations (in the form of controls / compliance)
- Roadmap

Possible recommendations can be technical, behavioral, or procedural in nature. The roadmap is the document in which the decision makers must make decisions.

In terms of a limited scope, security operations come up with an implementation plan that consists of four categories:

- Risks
- What threats precede the risks
- Which attack tactic could be used
- What attack technique could be used

Process from risk assessment to security operations (detection & monitoring)

The experts from the different companies described a process that is comparable to that of the others. It regards what the process from a risk assessment to security operations looks like. A risk analysis will be performed by a Security Operations Manager or risk department (risk managers, cybersecurity consultants). This is performed according to the process described earlier to have risk-based monitoring.

For certain risks that are identified, a monitoring and detection solution is required. The results and context information (results from the risk assessment) are communicated to security operations.

The communication that the experts described varies. Four out of the eleven experts described that after a risk analysis, the results are communicated to the security operations officer at the SOC. Because of the scope of the risk analysis (broadly and business), a technical deep dive is needed and performed with the engineering team. They will do the actual implementation of the use-cases in the SIEM; the monitoring solution. The security operations manager is

responsible for the translation towards an implementation. In addition, the engineering team is responsible for the technology. To do this translation, a consultation is needed. This could either be in meeting or chat form. During this meeting or chat, the consultant or security officer that performed the risk analysis discusses the results with the security engineer.

Afterwards the information is written down in an implementation plan. For example, it appears that a system has a certain authentication mechanism. Only one account can be used at a certain time. Thus, there is a need to monitor that account when an extra account tries to gain access or when someone tries to access the system outside the set times. This is discussed with the engineering team during the session.

Two out of the eleven experts described that the content engineer responsible for the technical implementation receives the risk analysis. This includes a list of the use-cases that must be implemented and the thresholds and context information. The project manager is responsible for the collection of the information needed and the translation to actual use-cases. The information that is collected is checked with the customer to determine if it complete and correct; if this is not, the case engineer will join in. The information is stored on a share for a specific customer.

Regarding the communication, one expert described that they do not see communication between the risk department and security operations often. A good start would be if the risk department would talk to the security operations site and explain what the risks are. They could also have a discussion to see how security operations can help them to reduce the risks to an acceptable residual risk. In the situation of the expert, the risk department comes up with certain compliances for which security operations have to implement a monitoring solution. They thus have their own way of coming to a monitoring solution because of the lack of communication and technical knowledge of the risk department.

Security operations translate the different risks and threats into use-cases that are implemented by the engineering team. To make this translation, the MITRE ATT&CK framework is used to map the risks and threats with the use-cases. If case information is missing, a technical deep dive is conducted to discuss technical details with the security officer and security engineer. Some experts state that the translation can be quite difficult because of the different languages and the knowledge gap between the risk analysis / risk department and security operations.

Information needs

The information needs for security operations will be described in two parts. To determine what kind of information is missing in the information exchange, this can be compared to the results of the risk analysis / threat modeling:

- **Implementing use-cases**

Based on the interviews, the experts responsible (engineering team) for implementing the different uses-cases / countermeasures in the SOC need the following information:

- Context information about the client (organization, strategy, goals, processes, network)
- Information about the risks and countermeasures
- What normal behavior is
- What abnormal behavior is
- What the different thresholds are
- What logfiles are available
- White and blacklisting

Not all information is delivered by default through the risk analysis. A part of the information is gathered through the process of implementing the monitoring solution for an organization and asking them for certain information when it is needed.

- **To respond to an attack**

The experts' states that analysts should be provided with the right information at the right time:

When a high alert occurs, the analyst wants to know: How often does it happen? What company is it? Which user does it concern? Do we know the IP Address? Different organizations use the monitoring service, so the analyst then receives an alert for some of their clients.

It is important to make sure that when a new organization makes use of the monitoring service, the analysts know where all the information can be found to react to an attack: the governance document, network, playbook, contact information, and use-cases. This information is shared in document management systems.

4.5 Gap description

In this section we will discuss, like described earlier, the gaps found in the literature and interviews. In this section, the following sub question will be answered:

SQ2: "What is missing in the information exchange between risk assessment / threat modeling and security operations?"

Translation of the risks / threats into use-cases

Six out of the eleven experts mentioned difficulties translating the different risks and threats into effective use-cases. The difficulty is how to translate a business risk into a technical measure because the goal is to reduce the risks of an organization. MaGMa (2017) stated that mapping compliance drivers to business drivers and use-cases could be an elaborate task. It is necessary that the things that are really linked to the risks of the organization are monitored. For example:

"We want to cover the business risks, we don't necessarily want to monitor the firewall because of that fact that you have a firewall. We want to monitor that firewall, but because you are afraid that someone will enter through that firewall and get to the data that you think is so important to you." [Interview 3 – Security Operations Manager SOC]

After performing the risk assessment / threat modeling for certain risks, a monitoring and detection solution is required, and the results and context information are communicated to security operations. Security operations translate these different risks and threats into use-cases, which are implemented by the engineering team. To make this translation, the MITRE ATT&CK framework is used to map the risks and threats with the use-cases.

One expert described that they often have problems when it comes to the gap between analysis and security operations. This occurs due to several factors. The main factor is the communication between the client and the consultant performing the analysis. The consultant translates their findings into a report. That report goes to the project leader and the project leader goes to work based on the input he receives. Then it could be the case that they did not quite understand each other on delivery. This can be addressed by, for example, communicating with each other earlier in the chain with the people that performed the risk analysis, and not waiting until the tests with the customer take place. This gap is partly caused by the knowledge

gap between risk assessment and security operations. This knowledge gap will be described in the next section.

Business / technical orientation (knowledge gap)

Five out of the eleven experts mentioned that there is a difference in orientation, which leads to a knowledge gap and a difference in languages.

When the risk analysis is performed, it could be possible that the risk analysis is more focused on the business risks. However, the engineering team needs technical information in order to implement certain countermeasures, for example use-cases in the SIEM, and to reduce these risks. SOC components (technical parts) are in that situation not really taken into account beforehand.

Regarding the information exchange, the results of the risk assessment are more oriented on business such as risks, threats, current measures, roadmap, and recommendations. Looking at needs of security operations, more technical information is needed to implement a monitoring solution for risks that require monitoring. It is important to have information relating to the business case, drivers, thresholds/baselines, rules/action/logic, logfiles, and information about the systems.

This mismatch, like earlier described, is partly caused by the different risk analysis methods that are used by risk managers and the SOC internally, which can give different results. In addition, there is a knowledge gap between the two. The risk analysis practitioners do not have the same technical knowledge to integrate technical components into the risk analysis that security operations need.

The focus of security operations is more on technology, so most of the time the technical risks are discussed. However, it is not always clear whether these technical risks are minimizing business risks or not. So, this also causes tension. On the other hand, because of the risk analysis being more business-oriented, it could lead to difficulties in the translation of the risks to a monitoring solution because of the technical information that is missing.

Monitoring / evaluation of risks and threats

Two out of the eleven experts described that the goal of monitoring and detection is to reduce and mitigate risks for an organization, and to be able to respond to eventual attacks. To see if

the monitoring is effective, risks, threats and use-cases have to be evaluated based on the input from the SOC to examine if extra controls or measures are needed. The SOC is responsible for providing the input for the security officer. This way, they can evaluate a certain risk. For example, the number of incidents and what kind of attacks occurred.

One expert stated that they talk to the customer about the changes in their environment every month to find out if the monitoring and use-cases have to be adjusted. Practice shows that it is very difficult, once it is implemented, to verify whether the risk increases or decreases. If a customer implements an extra preventive measure, the risk will be lower. However, in some cases security operations is not informed. Another expert stated that the number of false / positives makes it difficult to evaluate the risks and threats. None of the experts stated that they used Key Risk Indicators in their activities.

Use-case lifecycle

Two experts mentioned that one of the difficulties is the use-case lifecycle because threat scenarios change constantly.

"You are constantly working on the use-cases because use-cases change overtime, and the threat scenarios also change. So, in other words, if you implement a use-case for a customer, you question yourself whether these will still be relevant topics in a year or three / five years." [Interview 8 – Manager Blue Team]

At some point there is a decent existing set that has been built and this needs to be kept up to date, for example by adding new log files, changing threats. Thus, it is important that the risks, threats, and use-cases are evaluated overtime.

4.6 Proposal

In this section, based on the literature review and interviews, the following sub question will be answered:

SQ3: "What process or guidelines can be implemented to improve the information exchange between risk assessment / threat modeling and security operations?"

4.6.1 Guidelines and improvements

As was described earlier, the improvements identified during the interviews are:

- Joint exercises / common understanding
- Baseline
- Identify information needs

In general, most of the experts describe that a solution to this problem is quite difficult because of the earlier described knowledge gap and different orientation. It is important to create a common understanding between the two. The different practices need to be aligned by using a more concise way of onboarding a client. This includes the risk analysis method and the focus on the business and technical parts so that the different information needs from both sides are fulfilled. Based on the expert interviews and literature, the following guidelines and model can be implemented to bridge the earlier described gaps between the risk analysis and security operations.

Joint exercises

Six out of the eleven experts mentioned that one of the improvements to make the translation of the risks and threats identified within a technical solution (monitoring & detection) in a collaboration between risk assessment and security operations. There needs to be a conversation about the risks and threats identified, and how security operations could address those risks. In this way, a common understanding is created. The risk actors translate these risks into their risk management framework and in a technical monitoring solution (use-cases and alerts).

The practitioners performing the risk assessment have their own way of working and they are not just working with the security operations. It is difficult for them to really understand each aspect of the technical components and to focus on this in depth. As was described earlier, the requirements and controls that the risk managers propose can be too vague and broad. One expert stated:

"I think by starting to do joint exercises we can understand how risk management is doing what they are doing, and that they understand what we are doing and together we can put those things together." [Interview 10 – Security Operations Tech Lead SOC]

Baseline

Two of the experts described that a baseline could be implemented to automate the translation of risks into use-cases, for example based on the ISO standard. The ISO standard contains a description of the components that need to be monitored. This basic set of monitoring could be used to implement a basic set of use-cases. Client specific use-cases could then be implemented afterwards.

"So, it is really nice if you can automate a number of things, as long as you do not automate so far that you lose sight of the fact that it is really about mitigating those risks that you have identified at a strategic level." [Interview 9 – Director Business Security]

Identify information needs

Another improvement that two experts described is that after identifying the controls and countermeasures, there is need for a technical description. To do so, an agreement between the risk analysis and security operations can be made to describe what the different information needs are that match the two together. This identification of the information needs is performed earlier in section 4.5 and is also incorporated into the proposed model.

"There needs to be some kind of agreement in the middle. This is how much information we need, and this is what we need, because what I often see is, OK, we need to implement something for compliance and they say, OK, we checked the box, but they don't really know what we have done and if it is sufficient because they don't understand well enough the technical details to really know if that is sufficient or not." [Interview 10 – Security Operations Tech Lead SOC]

4.6.2 Model

Based on the literature review and grounded theory results (gaps and improvements) from the interviews conducted, we have designed a model to bridge the gap. First, we have looked at the current process derived from the Grounded theory (see section 4.3 and section 4.4 for the description). This way we could compare this with the proposed model to see the improvements and changes:

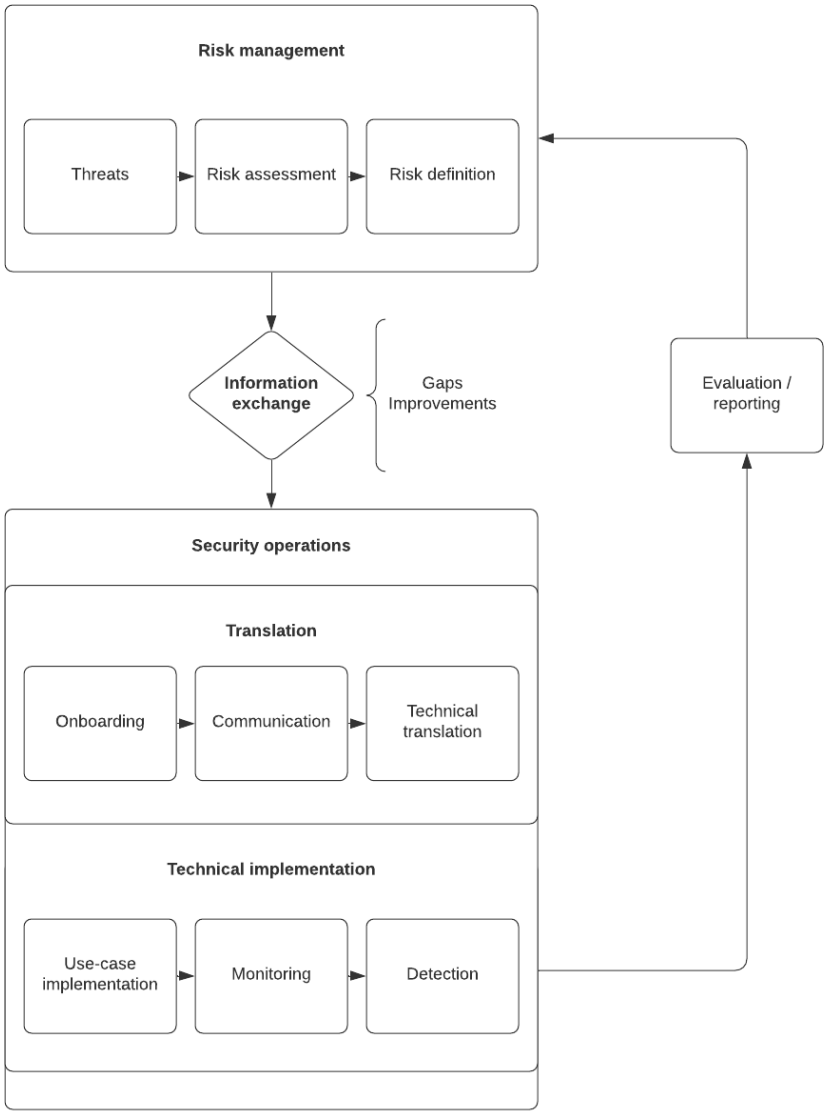

Figure 21: Current process based on Grounded theory (section 4.3 and section 4.4)

To improve the current situation, we looked at the identified gaps and improvements. The mayor improvements to bridge the gap are the joint exercises and the identification of the information needs. Compared to the current situation where there is no integral process of exchanging information, the proposed model contains exercises that need to be done in a collaboration instead of separate from each other:

- Translation
- Technical deep dive
- Evaluating & reporting

By performing these joint exercises between risk assessment and security operations, a common language can be created. Another improvement is the identification of information needs, which are incorporated within the process steps. The different topics that need to be discussed during joint exercises are based on the literature review and interviews. By discussing the topics, both information needs will be fulfilled to implement a monitoring solution that mitigates security risks for an organization.

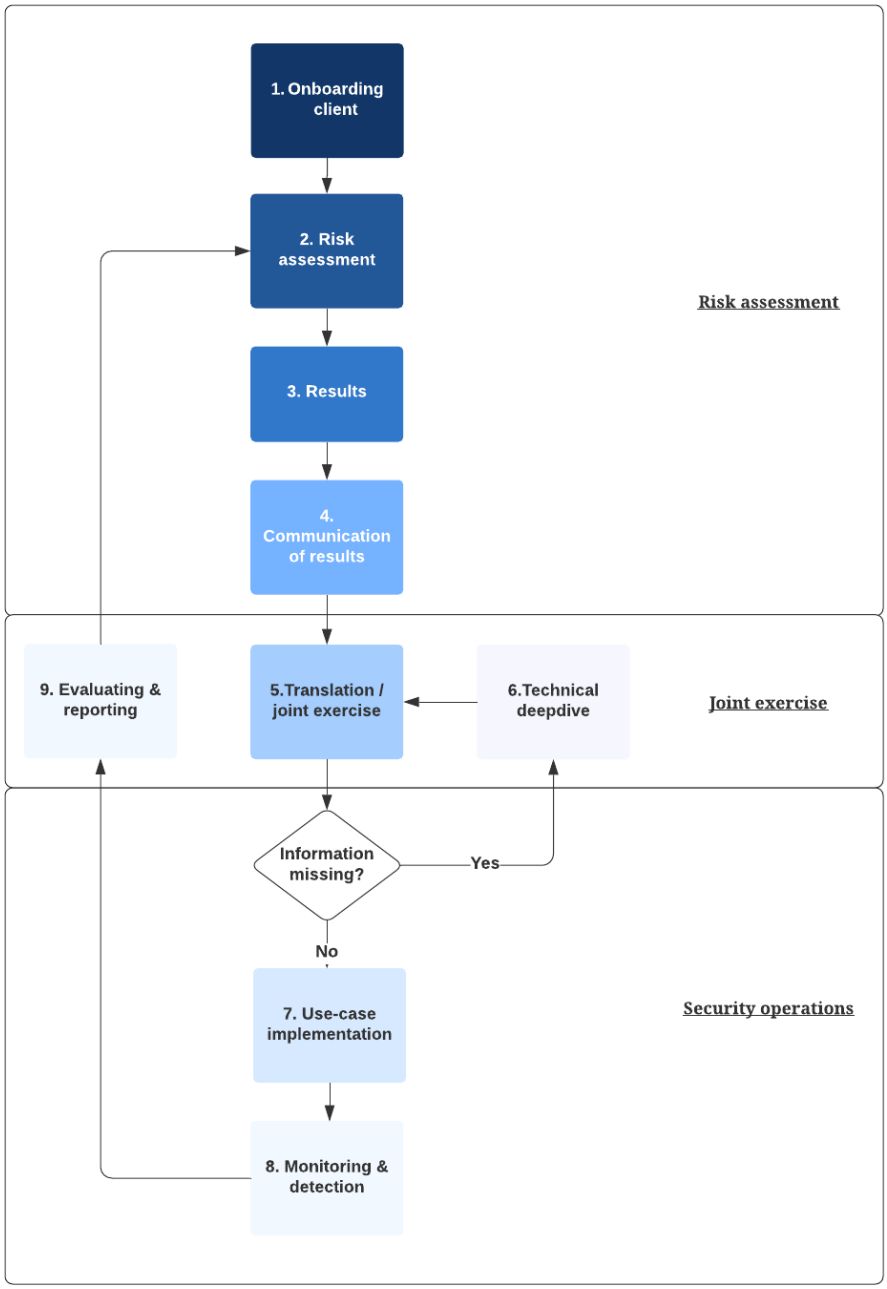

Figure 22: Model for bridging the gap between risk analysis and security operations monitoring and detection

The objective of this model is to improve the information exchange and communication channels between the risk and threat modelers and security operations to support both planners (risk managers and security developers) and first respondents in their activities. The people that participated in the risk assessment and threat modeling should provide information about the different risks and threats in such a way that security operations can implement controls and use-cases to monitor these and react if an actual attack occurs. To do so, risk assessment (RA) and security operations (SO) should perform joint exercises to come to a middle agreement. The model consists of nine steps to communicate and exchange the right information so that security operations can implement a technical solution to monitor and detect potential attacks.

1. **Onboarding client**

The first step of the model is to identify and understand an organization's business model, mission / vision, business objectives and assets to get an idea of what the organization and their environment look like.

2. **Risk assessment**

To onboard an organization for monitoring, it is necessary to think about business threats and risks before setting up a monitoring solution. First identify all cyber risks and quantify risks by determining the probability and the impact of a specific risk. This can be done by using a risk matrix for example. Secondly, look at the existing controls and their effect on the risks that are identified, and determine the potential impact of these. Finally, prioritize the identified risks.

3. **Results**

Then the results of the risk assessment need to be translated into a report containing the following subjects:

- Scope of the risk assessment.
- Risks / threats and the evaluation (probability / impact) (very low, low, moderate, high, or very high).
- Current measures.
- Recommendations (in the form of controls / compliances.
- The relevant information system names and location(s) and categorization.
- Description of the risk model and analytic approach.

- If the risk assessment includes organizational missions/business functions, describe the missions/functions.
- If the risk assessment contains information systems, also describe the system(s). For example, the missions and business functions the system is supporting, the information flows to and from the system(s), and the dependencies on other systems.
- A summary of the risk assessment results (tables / graphs).

4. **Communication**

Information security risks and related information must be communicated in a consistent manner with other types of risk communication within organization in order to be effective. The risk information can be shared via dashboards, briefings, reports and by updating repositories with risk related information and data. Documenting the sources of information about the risk assessment results supports the information sharing, because of the maintainability.

5. **Translation / joint exercise**

The translation of the risks and threats into a technical solution is a joint exercise between the people that have participated in the risk analysis and security operations. The goal is to acquire a common understanding and to complement each other in terms of business and technical knowledge.

The participants consist of risk managers, security operations manager, and security engineers.

To provide the information that security operations need and to bridge the gap, the following topics need to be discussed during the joint exercise between the risk analysts (risk assessment) and security operations:

- Context information about the client (business model, organization, strategy, goals, processes, network, systems) to give security operations an idea of the core business of the organization. Also, address the elements that are relevant to ensure that the use-case supports the business and vice versa. First, it should be made clear why the use-case is relevant for the business. In addition, it should also be made clear what the main drivers for the use-case are, for example: risk reduction, avoiding reputational damage

or financial loss, or compliance drives may apply. Another important part is who the main stakeholders are. Each stakeholder can have specific goals and interests.

- Information about the risks and current countermeasures (results of the risk assessment).
- It is important for the risks that have to be monitored that normal and abnormal behavior per risk is discussed. This way it can be used to translate this into rules (which detect and trigger alerts), logic (how events or rules will be considered), actions (which determine what action is required if logic or conditions are met), and the thresholds / baselines (when a use-case fires, for example: more than one login using the same ID).
- The location of the logfiles, so that it can be integrated within the SIEM. It is important to take the whole architecture into account.
- Regarding security incident response it is necessary to discuss what actions need to be taken when security monitoring alerts are fired, relating to a use-case. It is important to determine the appropriate response before implementing the use-case because significant added value from the SOC comes from incident response.
- For analysts it is very helpful to have some guidance on alert analysis generated by security monitoring rules. Such guidance will aid analysts in the correct interpretation of the security monitoring alert and to ultimately decide whether the alert is a genuine threat or a negligible event.

By gathering and discussing this information, security operations can map the risks with use-cases using the MITRE ATT&CK framework. Threat hunters, red teamers, and defenders use the MITRE ATT&CK framework to better classify threats and estimate an organization's risk. Risks and threats can be mapped with use-cases using this framework.

6. **Technical deep dive**

It could be the case that specific technical information is missing in the process, or that certain details must be discussed in a joint exercise with the people that performed the risk assessment and security operations to gather the right information for the implementation.

7. **Use-case implementation**

After translating the risks and threats into technical use-cases and defining the rules, actions, and logic the use-cases must be implemented. Security operations needs to integrate the identified data/log source into the SIEM. They need to look at the log files and need to identify

what is needed to detect an attack. While building this logic/rule for a use-case, it is important to identify the correct event field to perform correlation or aggregation. The defined logic and threshold in the use-case needs to be tested. By testing and tuning the use-cases potential noise can reduced. Based on the testing results, tuning will be required to ensure noise is reduced. When a use-case is implemented, the performance and alerts generated needs to be monitored by security operations to keep a check on false positives and overall health. After implementing the use-cases, all information is collected in a use-case repository, where context information and playbooks are stored.

8. Monitoring & detection

By implementing a use-case for a client, the analyst can detect and react to an actual attack and act according to the playbook. These playbooks are used to see what kind of actions are expected from the analyst handling the alert. Within the incident response process, roles and responsibilities for the use-case will also need to be described. By outlining the roles and responsibilities beforehand, security incident response can be carried out smoothly when incidents do occur.

9. Reporting & evaluation

The SOC reports trends and insights monthly to the security officer that is responsible so that they can re-evaluate the risks and determine if extra measures are needed. These trends and insights describe the statistics and output of the use-cases, and what kind of attacks occurred. Also, the reporting can be used to examine if the monitoring is effective in reducing risks for the organization. The output can be generic, like events and incident response, but can also be more specific. For example, specific reports may be created for this use-case. Such reports may even be differentiated for each stakeholder.

4.7 Feedback on the results

Due to the limited thesis project time, we conducted a series of interviews with experts to see if the model is realistic and practical. However, the best way the test the model, to determine the correctness of the model and to make possible changes, is to do so in a practical setting. Semi-structured interviews were conducted for the model and guidelines evaluation by presenting this to experts working in the field between risk assessment and security operations:

Interview	**RA/SO***	**Role**
1	SO	Security Operations Manager
2	SO	Strategic Advisor Cybersecurity
3	RA	Security Officer

Table 18: Participants feedback results

In total, three interviews with external experts, who did not participate in the interviews, were conducted asking the following questions:

1. What is the first impression of the model?
2. Is the model consistent with the current process of communication and information exchange?
3. Is the model understandable by going through the individual steps?
4. Is this model useful for the organization? Why?
5. What are the benefits of this model?
6. Are there certain elements irrelevant or overlapping in the process?
7. What are the limitations and weaknesses in the model? And what could be possible improvements for this?
8. Are there any other suggestions?

Before the interview, the results and model were sent to the experts so that that they could prepare for the interview. During the interview we presented the gaps and improvements that we found during the literature review and interviews, including the model that we built. The sections that were discussed were section 4.4 (general and gaps) and section 4.5 (improvement guidelines and model). After the presentation, the experts were asked if they could provide feedback: overall impression, strengths, and weaknesses so that this could be incorporated into

the final version. The interviews were not recorded or transcribed. By writing down the impressions, strengths, and weaknesses / improvements, the following summary could be given:

Overall

- Straightforward model with a good and familiar description of the gaps and the present gap in expectations.
- The model is understandable by going through the individual steps.
- It is compatible with the current process of communication and information exchange.

Strengths

- The model is clear and feedback heavy, useful for agreeing on the monitoring scope with the client.
- The model can easily be tweaked.
- The model simplifies the start of a process and standardizes a part of the onboarding and risk analysis. This prevents (expensive) customization that is difficult to manage in practice due to the diversity.

Weaknesses / improvements

- Expert 1 described that level 3 and 4 do not seem to be on the same "level" of importance.
- Another possible improvement is to provide more guidelines on how the joint exercise should be organized exactly. This includes what the important results are and what questions should be asked.
- Additional steps and topics of communication can be added. For example, expert 2 described that the difficulty with models is that the available log sources need to be identified. If risks are determined in this process of onboarding a client that needs to be monitored and mitigated, and the right log files to monitor this risk are not available, then the process must be redone.

Based on these strengths and weaknesses, the mode has been improved on two points:

- Log sources are added to the discussion topics.
- The topics for the joint exercises are more clearly stated, including who will participate and how the session should be organized.

Discussion

Based on the results, we can indicate that there is a gap between risk assessment and security operations in terms of communication and information exchange. This is in line with the study of (Osório, 2018), which also stated that there is a gap. However, the gap from (Osório, 2018) exists more in terms of SIEM's not providing an adequate security risk management, resulting in a gap between the SOC team and the business managers regarding the communication of security risk.

A similar gap is observed in the DevOps world. DevOps is a new emerging concept that many businesses are embracing as a solution to the division and barriers that exist between operations and software development today. Traditionally, software development was done in silos, separate from the systems operating. To bridge the gap, DevOps promotes collaboration and consistency by allowing implementation- and support teams to exchange baselines and data. DevOps allows a quick flow of scheduled tasks, including short deployment times. (Yarlagadda, 2018). The improvements that we propose to bridge the gap between risk assessment and security operations is similar, performing joint exercises together to share information and to create a common understanding about the risks and technical implementation.

5.1 Findings

In this section we will describe the mayor findings of our research:

Risk analysis results

When we compare the risk assessment results described by the experts with the guidelines mentioned in the NIST SP800-30) (NIST, 2012) for Tier 3, which is relevant for security operations, there is overlap (section 2.3). However, information about the information systems is missing (the missions and business functions the system is supporting, the information flows to and from the system(s), and the dependencies on other systems).

Information needs / gap

If we look at the descriptions of the information needs given by the experts and compare these to the guidelines of (MaGMa, 2017), we can see an overlap. Both describe a need for

information about the organization (purpose and drivers) and the technical implementation (rules, logfiles, logic, incident response, security analysis). However, based on the literature review and interviews, the risk assessment provides more business-oriented information in the form of processes, risks, threats, current measures, roadmap, recommendations, missing the more technical information.

This mismatch is partly caused by the different risk analysis methods that are used by risk managers and the SOC internally. This can produce different results. Also, there is a knowledge gap between the two. The risk analysis practitioners do not have the same technical knowledge to integrate technical components into the risk analysis that security operations need. This results into difficulties translating risks and threats into use-cases.

"There is often a gap between what the risk department is doing and what the SOC is doing. And that's because they do not speak the same language, so they don't understand each other. And I often see this as an issue." [Interview 10 – Security Operations Tech Lead SOC]

"*I remember once we had the compliance department requiring that we monitor all user activity. But what does that mean, we can't monitor all user activity*?" [Interview 10 – Security Operations Tech Lead SOC]

"How can we make that translation well once we have determined the controls? How can we carefully ensure that that translation is correct? We need to keep a very close eye on whether we really monitor the relevant risks and what the effect of this is? That is also the most difficult challenge, I think." [Interview 9 – Director Business Security]

Communication

In addition, in some cases we that there is a lack of communication. One expert described that often they do not see communication between the risk department and security operations. A good start would be if the risk department would talk to the security operations site and explain what the risks are. They could also have a discussion to see how security operations can help them to reduce the risks to an acceptable residual risk. In the situation of the expert, the risk department comes up with certain compliances for which security operations have to implement a monitoring solution. They thus have their own way of coming to a monitoring solution because of the lack of communication and technical knowledge of the risk department.

"There was no communication at all. So, I'm building a baseline based on my own assessment, looking at the threats, looking at the crown jewels and then deciding from there. So, there is sometimes no communication between them. And that's obviously not the ideal situation". [Interview 10 – Security Operations Tech Lead SOC]

Monitoring & evaluation

Based on the results, we can state that the goal of monitoring and detection is to reduce and mitigate risks for an organization and to be able to respond to eventual attacks. The SOC is responsible for providing the input for the security officer, so that they can evaluate a certain risk. Practice shows that it is very difficult to verify whether the risk increases or decreases once it is implemented. This is the case because the risk will be lower if a customer implements an extra preventive measure, but in some cases security operations is not informed. Also, the number of false / positives makes it difficult to evaluate the risks and threats.

During the literature review we saw that Key Risk Indicators is one of the major requirements for a risk assessment (Leversage and Byres, 2008). However, during the interviews, none of the experts stated that they make use of Key Risk Indicators in practice, which was unexpected.

Impact

What this means for the broader picture is that when the integrated process of risk assessment and security operations is done adequately, security operations can adequately mitigate the risks identified by the business lines. SOC reports on the implemented use-cases will support the information security team to accurately measure the effectiveness of their SOC services, and therefore the business risks.

Improvements

What we experienced during the interviews regarding the improvements is that it is difficult to find a solution to the gap between the risk assessment and security operations due to the earlier described knowledge gap. We proposed guidelines and built a model that helps to bridge the gap by doing joint exercises and identifying what information should be exchanged, and by using which communication channels. Cybersecurity firms can use these guidelines to improve the translation of the risk / threats into technical solutions, which contributes to the mitigation of risks identified during the risk assessment.

"I think by starting to do joint exercises we can understand how risk management is doing what they are doing, and that they understand what we are doing and together we can put those things together." [Interview 10 – Security Operations Tech Lead SOC]

"There needs to be some kind of agreement in the middle. This is how much information we need, and this is what we need" [Interview 10 – Security Operations Tech Lead SOC]

Feedback

During the feedback on the results, experts mentioned that the model simplifies the start of a process and standardizes a part of the onboarding and risk analysis. This prevents (expensive) customization that is difficult to manage in practice due to the diversity, which is interesting. This could mean that an expert from a consultant perspective is more interested in optimizing their effort, rather than achieving the best security for the client.

5.2 Threats to validity

To research the gap and find improvements for the information exchange we conducted a literature review and interviews with experts. To integrate both viewpoints we divided the experts into two groups: Risk assessment / threat modeling (RA) and security operations (SO).

The experts qualified based on role, experience, education and kind of organization. The goal was to have a distribution of 50/50 for each role and to interview practitioners from different companies. This way, due to different standpoints, views, and expressions, the generalizability of the findings would be improved. In the end we interviewed six experts from RA and five from SO, which matches the 50/50 distribution. For this research it was also important to interview experts that belong to an organization that provided security services to clients. Otherwise, because the process varies, this would have had a very distinct impact on the outcomes.

To analyze the qualitative data set, we applied a Grounded Theory like approach. To ensure that the data of the codebook are reliable, we performed partial double coding. This was done by letting an external individual code part of the qualitative data set, so that we could compare the different codes using the same steps. There were some disagreements about the different assignations of codes and where the codes were placed in the sentences. We took this into

account to improve the reliability. Our intention was also to perform interviewing, transcribing, and coding iteratively. This way, we would be able to determine when theoretical saturation was reached. Therefore, transcribing and coding started after the first interview was administered. Because coding took more time than anticipated, the process was not done fully iteratively.

Another limitation could be the theoretical saturation, which we did not reach because of the time constraints. Strauss & Corbin (1998) describe theoretical saturation as "The point in category development at which no new properties, dimensions, or relationships emerge during analysis". Potentially, we could have interviewed more experts to gather new potential insights, viewpoints, and valuable information.

In addition, the model should have been used for a period of at least a few months to come to a correct conclusion about the effectiveness of it. Potential weaknesses in practice can be identified during that period.

Finally, we interviewed a total of eleven experts. Five of these eleven experts were from one company and the other experts were external, which could have biased the results. We tried to minimize this by validating the results with experts from external companies who did not participate in the interviews, to improve the generalizability. After we described the gaps improvements, we built the model. Afterwards, we asked three external experts to provide feedback on the findings to improve the generalizability and to examine if the model is feasible and realistic. We incorporated this feedback within the model.

Conclusion

In this section we will reflect on the research objectives and research questions that have been formed. Furthermore, we will give recommendations for further studies.

With this research we contribute to the alignment of risk assessment with security operations to support them in their activities. The existing literature states that there is a gap between risk assessment and security operations. However, it does not prescribe, to the best of our knowledge, how the information exchange should be organized, fulfilling the information needs between risk assessment and security operations. In addition, available studies focus on proposing new solutions in the form of new tools, SIEM systems and risk managements systems, while not investigating how to improve the current practices and systems in organizations.

The objective of this thesis was to research and improve the information exchange and communication channels between the risk and threat modelers and security operations. We conducted qualitative research by conducting a literature review and eleven interviews. This led to an insight into the communication, information needs and what information is being exchanged. Based on this insight we could identify gaps within the information exchange and improvements. By using the insights from the literature review and results from the interviews we built a model that helps to bridge the gap between risk assessment and security operations, describing the information needs and communication. The model helps to support both planners (risk managers and security developers) and first respondents in their activities.

6.1 Summary of findings

For this research, the main research question was the following:

RQ: "What is the gap between risk assessment and security operations and how could this be improved?"

As technology continues to empower enterprises, the attack surface of organizations will continue to expand (Deloitte, 2020), this increases the need for cyber risk management and security operations to mitigate risks and threats, however based on the research we can

conclude that there is a gap between risk assessment and security operations due to different mindsets and knowledge.

This is the result of a different orientation of both exercises. Risk assessment focusses more on the business, and security operations more on the technical components. This results in a knowledge gap and different languages, which in turn results in a difficulty translating risks and threats into a technical solution.

It is important that security operations have the right information to their disposal regarding the business layer, the tactical layer, and the implementation layer. This way they are able to translation from a risk / threat to a technical implementation of a use-case. The main driver regarding the information gap is the earlier described knowledge gap between the risk assessment and security operations. This gap is due to their business and technical orientation. The risk assessment is business oriented and does not incorporate the tactical and implementation layer which regards the security monitoring and threat management.

The translation of risks and threats into use-cases is important. Security operations services the organization in pro-active monitoring and detecting intrusions, but also in responding and taking the correct measures to mitigate. The key is to synchronize the services to the business drivers to add value in protecting the business goals. The key inputs that drive the operational and financial results are the business drivers and activities. The SOC can translate the defined business drivers into their goals.

To bridge the gap, joint exercises can be performed to create a common understanding between the two and to identify the information needs. We implemented these improvements within the model.

6.2 Future research

Within this research, various directions for future research have been identified. The first direction is to use the model in a case-study to see how it functions in practice. Based on this case-study, potential weaknesses and limitations in practice can be identified and improved.

Another direction is to automate the translation of a risk / threat into a technical solution that could be implemented in the SIEM. By creating a baseline for a certain business sector based on methods and frameworks, for example ISO controls, a baseline for use-cases can be established. This basic set of monitoring could be used to implement a basic set of use-cases. Organization specific use-cases can be implemented afterwards. Further research is necessary to look at the different possibilities.

Finally, another interesting point for future research is the focus on the communication and information exchange in an organization that conducts risk assessment and security operations internally for their own organization. During this research we focused on organizations that provide security services for other organizations in the form of cyber risk management and security operations. It would be interesting to research how these processes differ from each other (process internally in comparison to providing services to other organizations).

Bibliography

Beasley, M. S., Branson, B. S., & Hancock, B. V. (2010). Developing Key Risk Indicators to Strengthen Enterprise Risk Management – How Key Risk Indicators can Sharpen Focus on Emerging Risk. Retrieved from https://www.coso.org/Documents/COSO-KRI-Paper-FullFINAL-for-Web-Posting-Dec110-000.pdf.

Bruce Schneier. Attack trees: Modeling security threats. *Dr. Dobb's journal*, December 1999.

Chittester C, Haimes YY. Risks of terrorism to information technology and to critical interdependent infrastructures. J Homel Secur Emerg Manag 2004;1(4):article 402.

Creswell, J.W., & Plano Clark, V.L. (2007). Designing and conducting mixed methods research. Thousand Oaks, CA: Sage Publications.

CSA Singapore. (2019, December). Guide to conducting cyber security risk assessment for critical information infrastructure. https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf.

CSA Singapore. (2021, February). Guide to cyber threat modeling. https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide-to-cyber-threat-modelling.pdf.

CyBOK, Burnap, P., & Rashid, A. (2019, October). *Risk Management & Governance Knowledge Area*. https://www.CyBOK.org/media/downloads/Risk-Management--Governance-issue-1.0.pdf.

CyBOK. (2019). *Security Operations & Incident Management Knowledge Area*. https://www.CyBOK.org/media/downloads/Security_Operations__Incident_Management_issue_1.0.pdf.

Davies, J., Finlay, M., McLenaghen, T., & Wilson, D. (2006). Key Risk Indicators – Their Role in Operational Risk Management and Measurement. In: ARM and Risk Business International, Prague, pp. 1–32. Retrieved from

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.893&rep=rep1&type=pdf.

Deloitte. (2020). *Future of the SOC Forces shaping modern security operations*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-deloitte-google-cloud-alliance-future-of-the-SOC-whitepaper.pdf

dos Santos Vilar Ferreira, L. M. (2017). *A multi-level model for risk assessment in SIEM*. https://repositorio.ul.pt/bitstream/10451/31288/1/ulfc123950_tm_Luis_Miguel_Ferreira.pdf.

Edgar, T. W., & Manz, D. O. (2017). Introduction to Science. *Research Methods for Cyber Security*, 3–56. https://doi.org/10.1016/b978-0-12-805349-2.00001-7.

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *E & i Elektrotechnik Und Informationstechnik*, *132*(2), 106–112. https://doi.org/10.1007/s00502-015-0289-2.

Galvanize. (2017). *KRI basics for IT governance*. https://www.wegalvanize.com/assets/white-paper-kris-it.pdf

Ghazouani, M., Faris, S., Medromi, H., & Sayouti, A. (2014). Information Security Risk Assessment A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications*, 103(8), 36–42. https://doi.org/10.5120/18097-9155

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*.

IBM. (2020, November 12). *A Quick Guide to Effective SIEM Use-cases*. Security Intelligence. https://securityintelligence.com/posts/quick-guide-to-siem-use-cases/

Ionita, D. (2013, July). *Current Established Risk Assessment Methodologies and Tools*. https://essay.utwente.nl/63830/1/MSc_D_Ionita.pdf.

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, 5(4), 87–88. https://doi.org/10.4103/0976-0105.141942

Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. *NIST*, 1–30. https://doi.org/10.6028/nist.sp.800-150

Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis 1981;1(1):1137.

Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., & Ahn, G.-J. (2019). Matched and Mismatched SOCs. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 1–5. https://doi.org/10.1145/3319535.3354239

Kosub, T. (2015, April). *Components and Challenges of Integrated Cyber Risk Management*. https://www.vwrm.rw.fau.de/files/2016/05/Cyber_Risk_2015-04-03.pdf

Leversage, Byres, 2008 D.J. Leversage, E.J. Byres Estimating a system's mean time-to-compromise *IEEE Secur Priv*, 6 (1) (2008), pp. 52-60.

MaGMa. (2017, November). A joint use-case framework from the Dutch financial sector. https://www.betaalvereniging.nl/wp-content/uploads/FI-ISAC-Use-Case-Framework-Full-Documentation.pdf

Makri, C., & Neely, A. (2021). Grounded Theory: A Guide for Exploratory Studies in Management Research. *International Journal of Qualitative Methods*, *20*, 160940692110136. https://doi.org/10.1177/16094069211013654.

Maheshwari, V., & Prasanna, M. (2016). Integrating risk assessment and threat modeling. *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2–3. https://doi.org/10.1109/inventive.2016.7823275

May, T. (2011). Social research: Issues, methods and research. London: McGraw-Hill International.

MITRE. (2018, April). *Cyber Threat modeling: Survey, Assessment, and Representative Framework.* https://www.mitre.org/publications/technical-papers/cyber-threat-modeling-survey-assessment-and-representative-framework

Naseer, H., Maynard, S. B., & Desouza, K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 1–30. https://doi.org/10.1016/j.dss.2020.113476

NIST. (2012). *Guide for Conducting Risk Assessments*. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Nweke, L. O. (2020). *A Review of Asset-Centric Threat modeling Approaches*. NTNU. https://thesai.org/Publications/ViewPaper?Volume=11&Issue=2&Code=IJACSA&SerialNo=1

Osório, A. M. S. (2018). *Threat Detection in SIEM Considering Risk Assessment*. https://repositorio.ul.pt/bitstream/10451/35434/1/ulfc121874_tm_Ana_Os%C3%B3rio.pdf

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology*, *52*(2), 137–145. https://doi.org/10.1037/0022-0167.52.2.137

Rizov, V. (2018). Information Sharing for Cyber Threats. *Information & Security: An International Journal*, *39*(1), 43–50. https://doi.org/10.11610/isij.3904

Rule, P. & John, V. M. (2015). A necessary dialogue: Theory in case study research. *International Journal of Qualitative Methods*, 1(11). DOI: 10.1177/1609406915611575.

Saini, V., Duan, Q., & Parachuri, V. (2008, April). *Threat modeling Using Attack Trees*. https://www.researchgate.net/publication/234738557_Threat_Modeling_Using_Attack_Trees

Gutierrez, D. (2021, June 16). Security and Risk Management Trends in 2021. SAP Blogs. https://blogs.sap.com/2021/06/15/security-and-risk-management-trends-in-2021/

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students, (6th ed.) London: Pearson.

Scarlat, E., Chirita, N., & Bradea, I. (2012). Indicators and Metrics Used in the Enterprise Risk Management (ERM). Economic Computation and Economic Cybernetics Studies and Research, no. 4.

S. Rass, “On game-theoretic risk management (part three) - modeling and applications,” 2017.

Strauss A, Corbin J. *Basics of qualitative research: grounded theory procedures and techniques*. Sage Publications, 1990.

Strauss, Anselm & Corbin, Juliet (1998) Basics of Qualitative Research: Techniques and procedures for developing grounded theory, Thousand Oaks,California: SAGE Publication.

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modeling approaches for APT-style attacks. Heliyo, 7(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969

Yarlagadda, R. T. (2018). Understanding DevOps & bridging the gap from continuous integration to continuous delivery. *Department of Information Technology, USA*. Published. https://www.researchgate.net/profile/Ravi-Teja-Yarlagadda/publication/350157935_Understanding_DevOps_bridging_the_gap_from_continuous_integration_to_continuous_delivery/links/6053df5e458515e83455a764/Understanding-DevOps-bridging-the-gap-from-continuous-integration-to-continuous-delivery.pdf

Zawiła-Niedźwiecki, J., & Byczkowski, M. (2009). Information Security Aspect of Operational Risk Management. *Foundations of Management*, *1*(2), 45–60. https://doi.org/10.2478/v10238-012-0010-2

Zimmerman, C. (2021). *Ten Strategies of a World-Class Cybersecurity Operations Center*. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.545&rep=rep1&type=pdf

Appendix A: Interview questions: Risk assessment / threat modeling & security operations

1. Do you give consent for the recording of the interview?
   - Purpose
   - How long the recording will be maintained (till I finish the thesis)
   - You can stop the interview any moment and request the interview to be deleted
   - I will transcribe the recording and anonymize it

2. How many years of experience in cyber security do you have?

3. What is your current role? And what does it involve in terms of activities and responsibilities?

4. Does your company provide services in terms of risk analysis and monitoring & detection to clients?

   - If yes, how does this process looks like – from risk analysis to the implementation to monitoring?

5. Which methods / techniques / frameworks do you use to perform risk assessment/ threat modeling to identify threats at a client? (ISO / NIST / ATTACK TREES / STRIDE / ATT&CK / PASTA for example)?

6. What are the results / kind of information that you get after performing these mapping exercises (RA / TM)? In terms of identified and the format of this information.

   - What actions are taken after the mapping exercises? To which persons do you communicate these findings? And how?

7. How does the process of longer-term monitoring of the identified threats and risks look like? To see if the measures are taken and if the threats are in control.

   - Do you use Key Risk Indicators to monitor this? If not, how do you monitor this?

   - And who is responsible?

8. Are there any activities that ensure communication of the risks to the SOC team in order to monitor this?

   - If yes, how is the information exchange organized with the SOC?

   - In what form and in what kind is the information being shared? (Meetings / Key Risk Indicators e.g.)

   - Which person receives the information?

   - If no, what is the reason and how could it be done?

9. Can you describe the relationship of risk assessment with security operations / SOC?

10. Do you use inputs from SOC for the risk assessment and threat modeling?
    - In terms of data about likelihood or specific events for example?
    - Anything else?

11. Do you implement the countermeasures like use-cases / rules for the SIEM yourself or does another colleague do this?
    - If yes, what kind of information do you need to do this?
    - If no, what kind of information do you think is needed?

12. Are you encountering problems / gaps in the process, communication between risk assessment and security operations?
    - If yes, can you explain?
    - What could be possible improvements?

13. Are you available for follow-up questions?

Interview questions: Security operations

1. Do you give consent for the recording of the interview?
    - Purpose
    - How long the recording will be maintained (till I finish the thesis)
    - You can stop the interview any moment and request the interview to be deleted
    - I will transcribe the recording and anonymize it

2. How many years of experience in cyber security do you have?

3. What is your current role? And what does it involve in terms of activities and responsibilities?

4. Does your company provide services in terms of risk analysis and monitoring & detection to clients?
    - If yes, how does this process looks like – from risk analysis to the implementation to monitoring?

5. We are now focusing on your role in the SOC/threat monitoring at a client. What kind of threat intelligence and threat models does the SOC receive?
    - Which of these intelligence sources are internal? And which external? (FireEye e.g.)

6. How do you receive information about risks & threats / controls / use-cases from risk assessment and threat modeling that have to be implemented for a client? How is information being exchanged?

7. How do you integrate the information from the risk management and threat modeling team into your processes?

    - E.g., are you tasked to implement recommended controls?
    - Do you have a way to consume the identified threat scenarios and monitor for those?

    - Do you receive any Key Risk Indicators for monitoring?

8. What kind of information do you need from risk management and threat modeling to improve the security operations and to be able to better respond to actual attacks?

    - In what kind of format?

    - Do risk assessment and threat modeling provide this information to implement reactive and corrective controls when an attack occurs? Is there anything missing?

9. Do you provide any data/information to the risk management and threat modeling team or participate in their activities?

    - (e.g., supply likelihood estimates, consult them on observed threats or recent threats from the threat intelligence feeds)?

10. Are you encountering problems / gaps in the overall process and communication itself with risk assessment?

    - If yes, can you explain?

    - What could be possible improvements?

11. Are you available for follow-up questions?

Appendix B: Coding (sub)categories & concepts

Category	Sub-category	Concept
Risk analysis	**Risk management**	Scope
Risk analysis	**Risk management**	Frameworks
Risk analysis	**Risk management**	Level
Risk analysis	**Risk management**	Preference
Risk analysis	**Risk management**	Profile
Risk analysis	**Risk management**	Scenarios
Risk analysis	**Risk management**	Methods
Risk analysis	**Risk management**	Providing input
Risk analysis	**Risk management**	Tunnel vision
Risk analysis	**Risk management**	Current measures
Risk analysis	**Risk management**	Sector
Risk analysis	**Risk management**	Report
Risk analysis	**Risk management**	Client
Risk analysis	**Risk management**	Knowledge
Risk analysis	**Risk management**	Method overlap
Risk analysis	**Risk management**	Focus
Risk analysis	**Risk management**	Context information
Risk analysis	**Risk management**	Stakeholders
Risk analysis	**Risk management**	Compliancy
Risk analysis	**Risk management**	Controls
Risk analysis	**Risk management**	Translation use-cases
Risk analysis	**Risk management**	Treatment plan
Risk analysis	**Risk management**	Measures
Risk analysis	**Risk management**	Platform
Risk analysis	**Risk management**	Deepdive technical
Risk analysis	**Risk management**	Integral process
Risk analysis	**Risk assessment**	Appetite
Risk analysis	**Risk assessment**	Evaluation
Risk analysis	**Risk assessment**	Identification
Risk analysis	**Risk assessment**	Analysis
Risk analysis	**Risk assessment**	Interval
Risk analysis	**Risk assessment**	Questions
Risk analysis	**Risk assessment**	Scope
Risk analysis	**Risk assessment**	Frameworks
Risk analysis	**Risk assessment**	Methods
Risk analysis	**Risk assessment**	Mismatch SOC
Risk analysis	**Risk assessment**	Own methods
Risk analysis	**Risk assessment**	Scope
Risk analysis	**Risk assessment**	Report
Risk analysis	**Risk assessment**	Controls

Risk analysis	**Risk assessment**	Measures
Risk analysis	**Risk assessment**	Audience
Risk analysis	**Risk assessment**	Level
Risk analysis	**Risk definition**	Technical
Risk analysis	**Risk definition**	Use-case mapping
Risk analysis	**Risk definition**	Insight
Risk analysis	**Risk definition**	Awareness
Risk analysis	**Risk definition**	Threats
Risk analysis	**Risk definition**	Profile
Risk analysis	**Risk definition**	Domains
Risk analysis	**Risk definition**	Definition
Risk analysis	**Risk definition**	Impact
Risk analysis	**Risk definition**	Probability
Risk analysis	**Risk definition**	Reduction
Risk analysis	**Risk definition**	Mitigation
Risk analysis	**Risk definition**	Owner
Risk analysis	**Risk definition**	Priority
Risk analysis	**Risk definition**	Net
Risk analysis	**Risk definition**	Key-risk indicators use
Risk analysis	**Risk definition**	Recommendation
Risk analysis	**Threats**	Intelligence
Risk analysis	**Threats**	Commercial
Risk analysis	**Threats**	Open-source
Risk analysis	**Threats**	Model
Risk analysis	**Threats**	Translation use-case
Risk analysis	**Threats**	Identification
Risk analysis	**Threats**	Priority
Risk analysis	**Threats**	Landscape
Risk analysis	**Threats**	Internal
Risk analysis	**Threats**	Feed
Risk analysis	**Threats**	Sharing
Risk analysis	**Threats**	Changing
Risk analysis	**Threats**	Evaluation
Risk analysis	**Threats**	Impact
Security operations	**Detection**	Account management
Security operations	**Detection**	Roles
Security operations	**Detection**	Strategy
Security operations	**Detection**	Vulnerability scans
Security operations	**Detection**	Implementation
Security operations	**Detection**	Incident management
Security operations	**Detection**	Work instructions
Security operations	**Detection**	Technical follow-up
Security operations	**Detection**	Own methods
Security operations	**Detection**	Information sharing
Security operations	**Detection**	Quality assurance
Security operations	**Detection**	Playbook

Security operations	**Detection**	Evaluation
Security operations	**Detection**	Ownership
Security operations	**Detection**	Reporting
Security operations	**Detection**	Collaboration
Security operations	**Detection**	Incident context information
Security operations	**Detection**	Automation
Security operations	**Detection**	Tooling
Security operations	**Detection**	IDS
Security operations	**Detection**	Governance
Security operations	**Detection**	Integral services
Security operations	**Detection**	Improvement
Security operations	**Monitoring**	Translation requirements
Security operations	**Monitoring**	Impact evaluation
Security operations	**Monitoring**	Focus
Security operations	**Monitoring**	Reporting
Security operations	**Monitoring**	Risk-based
Security operations	**Monitoring**	Behavior
Security operations	**Monitoring**	Variants
Security operations	**Monitoring**	Communication
Security operations	**Monitoring**	Providing input
Security operations	**Monitoring**	Effectivity
Security operations	**Monitoring**	Scope
Security operations	**Monitoring**	Analyst
Security operations	**Monitoring**	Alerts
Security operations	**Monitoring**	Baseline
Security operations	**Monitoring**	Documentation
Security operations	**Monitoring**	Context information
Security operations	**Monitoring**	SIEM
Security operations	**Monitoring**	Use-cases
Security operations	**Monitoring**	IOC
Security operations	**Use-case implementation**	Translation
Security operations	**Use-case implementation**	Mapping
Security operations	**Use-case implementation**	Logfiles
Security operations	**Use-case implementation**	Baseline
Security operations	**Use-case implementation**	Framework
Security operations	**Use-case implementation**	Engineering
Security operations	**Use-case implementation**	Resources
Security operations	**Use-case implementation**	Repository
Security operations	**Use-case implementation**	Client information
Security operations	**Use-case implementation**	Implementation
Security operations	**Use-case implementation**	Information follow-up
Security operations	**Use-case implementation**	Reporting output
Security operations	**Use-case implementation**	Effectiveness
Security operations	**Use-case implementation**	Evaluation
Security operations	**Evaluation / reporting**	Monitoring influence
Security operations	**Evaluation / reporting**	Risks

Security operations	**Evaluation / reporting**	Threats
Security operations	**Evaluation / reporting**	Use-cases
Security operations	**Evaluation / reporting**	Reporting
Security operations	**Evaluation / reporting**	Effectivity
Security operations	**Evaluation / reporting**	Client
Security operations	**Evaluation / reporting**	Cyclus
Security operations	**Evaluation / reporting**	Responsibility
Translation	**Onboarding**	Motivation
Translation	**Onboarding**	Risk analysis input
Translation	**Onboarding**	Time
Translation	**Onboarding**	Scope (difficulty)
Translation	**Onboarding**	Document
Translation	**Onboarding**	Use-cases
Translation	**Onboarding**	Threat scenarios
Translation	**Onboarding**	Context information
Translation	**Onboarding**	Functionality
Translation	**Onboarding**	Questions
Translation	**Onboarding**	Project management
Translation	**Onboarding**	Information sharing
Translation	**Onboarding**	Motivation
Translation	**Technical translation**	Risks
Translation	**Technical translation**	Threats
Translation	**Technical translation**	Use-cases
Translation	**Technical translation**	MITRE framework
Translation	**Technical translation**	Engineering
Translation	**Technical translation**	Technical-deepdive
Translation	**Technical translation**	Requirements
Translation	**Technical translation**	Method
Translation	**Technical translation**	Collaboration
Translation	**Technical translation**	Responsibility
Translation	**Technical translation**	Engineer
Translation	**Technical translation**	Security Operations Manager
Translation	**Communication**	Collaboration
Translation	**Communication**	Meetings
Translation	**Communication**	File share
Translation	**Communication**	Presentation
Translation	**Communication**	Stand-up
Information exchange	**Gaps**	Misunderstanding
Information exchange	**Gaps**	Collaboration
Information exchange	**Gaps**	Language difference
Information exchange	**Gaps**	Resources
Information exchange	**Gaps**	Use-case lifecycle
Information exchange	**Gaps**	Two-way (departments)
Information exchange	**Gaps**	Methods used
Information exchange	**Gaps**	Translation difficulty

Information exchange	**Gaps**	Governance
Information exchange	**Gaps**	Reporting
Information exchange	**Gaps**	Consistency
Information exchange	**Gaps**	Effectivity insight
Information exchange	**Gaps**	Knowledge gap
Information exchange	**Improvements**	Language overlap
Information exchange	**Improvements**	Joint exercises
Information exchange	**Improvements**	Middle agreement
Information exchange	**Improvements**	Identify information needs
Information exchange	**Improvements**	Method overlap
Information exchange	**Improvements**	Common understanding
Information exchange	**Improvements**	Baseline
Information exchange	**Improvements**	Difficult