Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Synne Bakke Kjærvik

Utilization of ServiceNow's Risk Management Functionality Within the GRC Module

A Case Study

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Camilla Olsen
July 2023

NTNU
Norwegian University of Science and Technology

Synne Bakke Kjærvik

Utilization of ServiceNow's Risk Management Functionality Within the GRC Module

A Case Study

Master's thesis in Communication Technology and Digital Security
Supervisor: Maria Bartnes
Co-supervisor: Camilla Olsen
July 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Title: Utilization of ServiceNow's Risk Management Functionality Within the GRC Module: A Case Study

Student: Synne Bakke Kjærvik

Problem description:

Effective risk management is essential for organizations to make informed decisions, achieve their goals and protect themselves from unforeseen events. This involves identifying, assessing, and prioritizing potential risks, and developing and implementing strategies to minimize or mitigate their impact. Traditional risk assessments using Excel sheets and Word documents may result in ineffective risk management due to their limitations in providing a comprehensive view of the overall risk landscape. Performing data analysis and reporting manually is time-consuming and increases the chances of errors and inconsistencies.

The Governance, Risk, and Compliance (GRC) module in the ServiceNow platform may help organizations streamline their risk management processes and enhance their risk management capabilities, ensuring that it is accessible and usable for all relevant stakeholders. Furthermore, a risk library can help provide a centralized, structured, and consistent approach to risk management. By providing a pre-configured set of risk categories, definitions, and assessment methodologies, it can help reduce the complexity and time needed to configure and customize the GRC module. This can also help ensure consistency and accuracy in risk assessments and reporting.

This project aims to explore the effectiveness of utilizing the GRC module in ServiceNow for risk reporting, and to what degree a risk library can contribute to enhancing this process. A risk library must comply with applicable regulations and standards and capture potential risks through a thorough understanding of the risk landscape. To investigate, a literature review of relevant material will be conducted, along with interviews aimed at evaluating the impact of the GRC module on various aspects such as risk reporting and decision support, and exploring challenges of risk management. Ultimately, the goal of the project is to contribute to the understanding of the potential benefits and limitations of using ServiceNow and risk libraries for risk management in organizations, and whether it can address identified challenges.

Approved on: 2023-03-17
Main supervisor: Maria Bartnes, NTNU
Co-supervisor: Camilla Olsen, Sopra Steria

Abstract

In an era of increasing complexity and risk, the management of governance, risk, and compliance (GRC) within organizations is more critical than ever. This thesis examines the potential of ServiceNow's GRC module and a standardized risk library in solving challenges in traditional risk management and enhancing GRC processes. Through a qualitative research approach consisting of semi-structured interviews, the study provides insightful perspectives on utilizing ServiceNow's GRC module, implementation considerations, and the potential of a standardized risk library to enhance risk management processes.

The findings suggest that ServiceNow's GRC module fosters improved risk visibility, enhanced decision-making, and workflow efficiency, bolstering the organization's risk management framework. Additionally, including a standardized risk library introduces a consistent, structured, and efficient method of risk identification, assessment, and prioritization. Nevertheless, successful implementation depends on factors such as organizational readiness, stakeholder engagement, clear goal definition, and extensive user training.

The study's main limitation lies in the small sample size of interviewees, potentially inducing bias in the findings. Nevertheless, the research provides valuable insights into the adoption and potential of GRC tools like ServiceNow in strengthening risk management processes in organizations.

Sammendrag

I en tid med økende kompleksitet og risiko, er styring av governance, risk, and compliance (GRC) innen organisasjoner mer kritisk enn noen gang. Denne masteroppgaven undersøker potensialet til ServiceNow's GRC-modul og et standardisert risikobibliotek for å løse utfordringer i tradisjonell risikostyring og forbedre GRC-prosesser. Ved bruk av en kvalitativ forskningsmetode bestående av semi-strukturerte intervjuer, gir studien verdifull innsikt i bruken av ServiceNow's GRC-modul, hensyn ved implementering, og potensialet til et standardisert risikobibliotek for å forbedre risikostyringsprosesser.

Funnene antyder at ServiceNow's GRC-modul fremmer forbedret risikosynlighet, forbedret beslutningstaking og effektivitet i arbeidsflyt, og styrker organisasjonens risikostyringsrammeverk. I tillegg introduserer et standardisert risikobibliotek en konsekvent, strukturert og effektiv metode for risikoidentifikasjon, vurdering og prioritering. En vellykket implementering avhenger imidlertid av faktorer som organisatorisk beredskap, engasjement fra interessenter, klar måldefinisjon, og omfattende brukeropplæring.

Oppgavens hovedbegrensning ligger i et lite utvalg av intervjuobjekter, noe som potensielt kan indusere skjevhet i funnene. Likevel gir oppgaven verdifulle innsikter i adopsjon og potensialet til GRC-verktøy som ServiceNow for å styrke risikostyringsprosesser i organisasjoner.

Preface

This thesis is the final submission for the MSc. in Communication Technology and Digital Security, and concludes my studies at the Norwegian University of Science and Technology (NTNU). The research was conducted from February to July 2023.

I want to thank my supervisors, Maria Bartnes and Camilla Olsen, for their guidance over the past semester. Furthermore, I would like to thank Jakob Vagle at Sopra Steria for his invaluable insights and help on the ServiceNow platform. A big thank you is also directed to the interview participants, who took the time to share their expertise in the research area. It is greatly appreciated, and without it, the thesis would not have been possible to carry out.

Finally, I would like to thank friends and family for the love and support you have given me during the project. Your encouragement has been a great help when things have felt frustrating. An extra thank you is directed to my sister for taking the time to proofread the thesis.

Synne Bakke Kjærvik

Trondheim, July 2023

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Effective risk management has never been of greater importance [HDLL20]. The limitations of conventional risk management techniques become more apparent as today's risk landscape becomes more complex due to globalization, digitization, regulatory changes, and other global events [MC17; Bea17; ATRC19]. This scenario has driven the need to explore the potential of more advanced, technology-driven approaches [Pri22; KPM23] such as the Governance, Risk, and Compliance (GRC) module from ServiceNow [Serc; Sera; Serd]. GRC solutions manifest technological advancement in risk management, a significant trend that necessitates comprehensive academic exploration. Thus, this thesis contributes to the academic discourse by investigating potential benefits and drawbacks, providing valuable insights to scholars and practitioners alike.

Additionally, the research discusses how manual operations, which are frequently time-consuming and error-prone, dominate traditional risk management processes [AF20]. The thesis hypothesizes that a standardized risk library, in tandem with ServiceNow's platform, can streamline these processes and improve efficiency, potentially reducing human error and inconsistencies.

The thesis holds practical implications for organizations contemplating the adoption of an integrated GRC platform and a standardized risk library. The findings can serve as a valuable reference point, guiding organizations to make more informed decisions. In essence, the relevance of this thesis extends beyond academic advancement, potentially informing business practices and responding aptly to the evolving demands of risk management in our increasingly complex and dynamic business environment [WJ13].

ServiceNow was named the World's Most Innovative Company in 2018 by Forbes [For18], ranking the 100 firms investors think are most likely to generate big, new growth ideas. Still, little research has been published about the ServiceNow platform. In 2020 [SBJ+20], an article about using ServiceNow in conjunction with the

Prometheus and Grafana platforms for monitoring and event response management for future pre-exascale systems at the Lawrence Berkeley National Laboratory's National Energy Research Scientific Computing Center (NERSC) was published. Besides this, little research exists, particularly on the GRC module. Therefore, this thesis contributes to bridging the current knowledge gap.

1.1 Objectives

This thesis explores the potential effectiveness of advanced risk management solutions in addressing the limitations and challenges associated with traditional risk management methods, specifically the GRC module in the ServiceNow platform and incorporating a standardized risk library.

The study aims to evaluate the capacity of these solutions to streamline risk management processes, enhance reporting capabilities, and improve decision-making and compliance efforts within organizations. It seeks to provide a nuanced understanding of these systems' benefits and potential drawbacks, thus offering valuable insights for both academic and practical applications. Through a literature review and insightful interviews, the research investigates whether integrating ServiceNow's GRC module and a standardized risk library can contribute to a more comprehensive, efficient, and consistent approach to risk management.

1.1.1 Research Questions

Based on the objectives, three research questions have been composed. These will be elaborated on in the following sections.

RQ1: What are some common limitations and challenges with traditional risk management?

The first research question aims to identify and understand traditional risk management practices' typical limitations and challenges. Traditional risk management, characterized by manual processes often managed in spreadsheets, has been the cornerstone for many organizations. However, the rapidly changing business environment and increasing risk complexity necessitate reviewing these traditional methods. Despite their prevalence, these methods often have inherent challenges that may affect risk management's efficiency, accuracy, and comprehensiveness. This question delves into these challenges, providing a foundation to examine how modern risk management solutions may address these limitations. Understanding these challenges is crucial as it informs the areas where improvement and innovation are most needed, setting the stage for exploring contemporary solutions to these longstanding issues.

RQ2: To what extent could the use of ServiceNow's GRC module help solve these challenges?

The second research question seeks to determine whether the GRC module can help overcome the challenges identified with traditional risk management methods. As organizations strive for efficiency and accuracy in their risk management processes, adopting advanced platforms becomes a discussion point. This research question will explore the practicalities of using the GRC module, its efficacy in risk reporting and decision support, and its role in streamlining risk management processes.

RQ3: How can a standardized risk library contribute to enhancing this process?

The third research question delves into the potential of a standardized risk library for optimizing risk management processes, particularly in conjunction with the GRC module. It aims to explore how a risk library, with pre-configured risk categories, definitions, and assessment methodologies, can contribute to streamlining risk management practices. This question will examine how it can align with the GRC module to enhance risk management and whether a standardized risk library can contribute to overcoming the limitations of traditional risk management methods.

1.2 Limitations

This thesis is not without limitations. The conclusions of this thesis are based on two interviews, which is one such limitation. While these interviews provide vital firsthand insights into the experience of utilizing ServiceNow's GRC module and a risk library, the scope is inherently limited. They represent the experiences and perspectives of a limited sample size and may not represent the diversity of experiences and perspectives across organizations and industries. Potential bias also constitutes a limitation. As the participants have implemented and utilized the GRC module and a risk library in their organizations, their perspectives may be positively biased toward these tools due to their personal experiences or the organization's investment in these technologies.

The focal point of this thesis is another restriction. Implementing ServiceNow's GRC module and a standard risk library for risk management is the explicit focus of this thesis. While these instruments represent the trend toward digitalized risk management solutions, they are only a subset of the numerous technologies available in this field. Therefore, the findings and conclusions may only apply to a subset of risk management tools. In addition, this thesis provides a snapshot of the field of risk management at a particular period. Given the rapid evolution of digital technology, the applicability and precision of the findings may shift as new technologies and

methodologies emerge. This thesis offers a limited view of the current landscape due to its temporal restriction.

Lastly, the absence of experimental or quantitative data represents a substantial limitation. This thesis significantly relies on qualitative information gleaned from interviews and literature reviews. Quantitative studies or experimental data could provide additional objectivity and the ability to quantify the impact or efficiency of the GRC module and risk library.

Despite these limitations, this thesis provides a crucial foundation for understanding the potential benefits and challenges of implementing advanced risk management solutions, such as ServiceNow's GRC module and a standard risk library. The insights from this research can guide future studies and practical implementations, contributing to the continuous evolution and improvement of risk management practices.

1.3 Outline of Thesis

The thesis is structured as presented here:

Chapter 2: Background includes insight into risk management and ServiceNow's GRC module.

Chapter 3: Methodology explains the methodology of the project.

Chapter 4: Results presents the findings from the performed interviews.

Chapter 5: Discussion contextualizes the findings with the literature study conducted and discusses how they can shed light on the research questions.

Chapter 6: Conclusion and Future Work concludes the thesis and presents suggestions for future work within the topic.

Chapter 2
Background

This chapter presents background information relevant to this thesis. This includes an overview of the context and key concepts related to risk management and a thorough look at ServiceNow's GRC module.

2.1 Risk Management

Risk management is the systematic process of identifying, assessing, and prioritizing risks, defined as "the effect of uncertainty on objectives" [Int22], associated with business operations and activities, followed by developing and implementing strategies to minimize the impact of those risks [Int18; Int22]. Risk management is central to any organization's strategic management [HT21; RS23]. It is an integral element of general management practice and essential for the survival and growth of any organization, as it enables the anticipation and mitigation of potential threats to their operations, financial stability, or reputation. Economic uncertainties, legal liabilities, strategic management errors, accidents, and natural disasters are potential risks in this context. In addition, they may be specific to particular industries or regulatory environments [Hub10]. Understanding and managing these risks is essential for protecting an organization's assets and assuring the successful execution of its strategic and operational objectives [Int18].

The role of risk management in organizational decision-making is crucial [KPM23]. It provides a structured method for comprehending and addressing uncertainties [KM12]. Through the risk management process, decision-makers can comprehend the potential repercussions of various risks, rank them according to their likelihood and severity, and determine the most effective strategies for mitigating them [Int22; Int18]. This may involve accepting the risk, transferring it, minimizing its impact, or altogether averting it. With this knowledge, organizations can make decisions that balance prospective risks and rewards [HT21]. Risk management also includes compliance with laws and regulations, essential for sustaining the organization's legal

and ethical integrity, protecting its reputation, and avoiding potential fines and legal repercussions [MK15].

Effective risk management involves more than simply preventing losses. It involves achieving the mission and objectives of the organization, promoting efficiency and effectiveness, ensuring compliance, and facilitating informed decision-making and strategic planning.

2.1.1 Risk Management Process

The purpose of risk management is to create and protect value. Risk management enhances performance, encourages innovation, and supports achieving goals [Int18]. Risk assessments are performed in virtually every organization, and the size and scope vary greatly. This variation occurs across industries, organization sizes, and even within different business areas across a specific organization [Ser23c; SAY13].

The ISO 31000 "Risk Management – Guidelines" [Int18] and ISO 27005 "Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks" [Int22] standards give an overview of the full risk management process. The principles outlined guide the characteristics of effective and impactful risk management, communicate its value and explain its intent and purpose, and should be considered when establishing the framework and processes for an organization's risk management. Figure 2.1 illustrates the risk management process. Each step will be elaborated on in the subsequent sections.

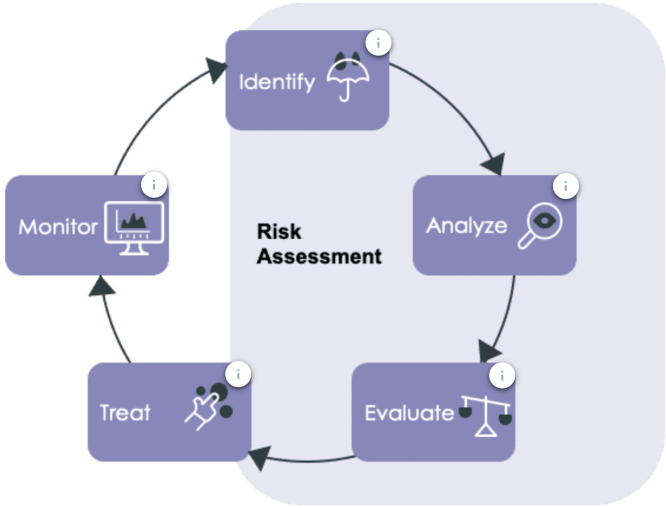


Figure 2.1: Risk Management Process [Ser23a]

Risk Identification

Risk identification aims to identify, recognize, and describe risks that can help or hinder an organization from achieving its objectives. Relevant, suitable, and current information is essential in this phase [Int18]. The purpose is to generate a catalog of the risks that could potentially harm the organization [Int22].

Organizations must consider multiple factors and their interactions when identifying hazards. These include understanding the origins of risk (whether tangible or intangible), identifying trigger factors and events, assessing potential threats and opportunities, evaluating existing vulnerabilities and capabilities, monitoring changes in the external and internal environments, recognizing indicators of imminent risks, understanding the characteristics and value of assets and resources, predicting possible outcomes and their impact on goals, and acknowledging lagging indicators [Int18]. Regardless of the organization's ability to regulate risk sources, it is essential to identify risks [SAY13]. Multiple outcomes may result in diverse tangible or ineffable consequences [WJ13].

Risk Analysis

Risk analysis aims to comprehend the nature of risk, including its characteristics and the appropriate level of risk [Int18]. It evaluates various factors, including uncertainty, risk sources, consequences, probability, events, scenarios, controls, and their effects. Events can have multiple causes and repercussions, potentially impacting diverse objectives [WJ13]. A risk analysis's level of detail and complexity depends on the information's objective, availability, accuracy, and resources [Int18; WJ13]. Organizations may employ qualitative or quantitative approaches, or a combination of the two, depending on the circumstances and intended application of the analysis. Embedding risk analysis within an effective infrastructure ensures its results are accepted and acted upon [Wil93].

During the process of risk analysis, multiple significant factors come into play. Evaluating the likelihood of events and their outcomes is essential to assess the prospective risks [Int18; Int22]. Understanding the nature and variety of consequences enables the identification of various potential impacts. In addition, considering complexity and interrelationships enables a comprehensive comprehension of how elements of the risk landscape interact [Int18]. Additionally, time-dependent factors and volatility must be considered, as they can substantially affect the potential risks. Evaluating the impact of existing controls assists in determining their efficacy in mitigating risks. Last, recognizing sensitivity and statistical reliability enables a more precise evaluation of the potential hazards.

Diverse opinions, biases, risk perceptions, and judgments can affect risk analysis

[Ave15]. In addition, the quality of the information utilized, the assumptions made, any omissions, and the limitations of the analysis methods and their implementation can all impact the reliability and accuracy of the risk analysis [Int18]. Consequently, these influencing factors must be evaluated, documented, and communicated to decision-makers. Quantifying highly uncertain events, particularly those with severe consequences, can be difficult. In such situations, combining various analysis techniques yields a more comprehensive comprehension and deeper insights into the associated risks. Risk analysis results play an essential role in risk evaluation, allowing organizations to determine the need for risk management and influencing the selection of suitable strategies and methods [Int18]. These insights are especially useful in decision-making processes where alternative options present varying types and levels of risk, enabling organizations to make informed decisions based on a comprehensive understanding of potential risks.

Risk Evaluation

Risk evaluation intends to facilitate decision-making procedures, and it entails comparing the results of a risk analysis to predetermined risk criteria to determine whether additional measures are required [Int18]. Risk evaluation may result in decisions such as deciding not to take any additional steps, considering alternative risk management options, conducting additional analysis to comprehend the risk better, maintaining existing controls, or reevaluating objectives. When making decisions, it is essential to consider a broader context and the actual and perceived consequences for both external and internal stakeholders. The outcomes of risk evaluation should be documented, communicated, and validated at the appropriate organizational levels [Int18].

Risk Treatment

Risk treatment is the process and the implementation of tools to modify risk, including tools to avoid, reduce, optimize and transfer risk. How one chooses to treat risk will depend on which type of strategy the organization has in place for risk management [Ave15]. Choosing the most appropriate alternatives for risk treatment involves weighing the potential benefits derived from goal achievement against the costs, effort, or disadvantages of implementation [Int18]. When choosing, the organization should consider stakeholders' values, perceptions, and potential engagement, as well as the most appropriate ways to communicate with them and consult them.

Risk treatment encompasses various alternatives that organizations can employ [Int18]. For instance, risk can be managed by avoiding it entirely, such as deciding not to proceed with an activity with potential risk. Conversely, an organization might choose to take on or even increase risk in pursuit of an opportunity. Managing risk can also involve eliminating the source, modifying the likelihood of occurrence,

or altering the potential consequences. Additionally, risk sharing can be achieved through contracts or insurance purchases. In certain cases, retaining the risk may be the most appropriate course of action, provided that it is a carefully considered decision [Int18].

The risk treatment process involves considering all of the organization's obligations and voluntary commitments, as well as the perspectives of stakeholders. When choosing among the alternatives for risk treatment, decisions should be aligned with the organization's goals, defined risk criteria, and available resources [Int18].

Risk Monitoring

Continuous monitoring is considered an important factor that enables quick responses to risks, vulnerabilities, and threats that any organization might face in daily life [AWV20]. Monitoring and review aim to ensure and improve the quality and effectiveness of the process design, implementation, and outcomes [Int18]. Monitoring and review must be an integral part of the risk management implementation to ensure that the various forms of treatment remain effective. Ongoing monitoring and regular review of the risk management process and its outcomes should be a planned part of the risk management process with clearly defined responsibilities [Int18].

Monitoring and review should occur at all process stages [Int18]. It involves planning, collecting, and analyzing information, recording results, and providing feedback. The results of monitoring and review should be integrated into the organization's performance management, measurement, and reporting activities throughout the organization [Int18; Int22].

2.2 Evolution of Risk Management

The evolution of risk management practices is a testament to the increasing complexities of business environments, rapid advancements in technology, and the continuously changing regulatory landscape [MK15]. Risk management has traditionally been viewed as a siloed, reactive function [KPM23]. Recognizing risks originating from diverse areas like operations, reputation, strategy, and environment has broadened the scope of risk management [HT21].

As technology advances, businesses leverage it to manage risks effectively [Pri22]. The shortcomings of traditional, manual tools like Excel spreadsheets and Word documents have pushed organizations towards more technologically sophisticated risk management solutions [ZR08]. These solutions offer automation capabilities, streamlining risk identification, assessment, and response processes while reducing the likelihood of manual errors. Moreover, these technologies facilitated the consolidation

of risk data, enabling an integrated view of the risk landscape across the organization [BMNR15; ASM23].

Adopting an Integrated Risk Management (IRM) approach reflects the shift towards a holistic approach where all risks are identified, assessed, and managed in an integrated manner rather than in isolation, promoting interdepartmental communication and strategic decision-making [HT21; Ser23c; RS23; KPM23]. Modern risk management practices incorporate predictive analytics, machine learning, and artificial intelligence to identify emerging threats and predict their potential impact [GNW12]. This shift towards proactive risk management marks a significant transformation from the reactive nature of traditional risk management practices [Ave15].

The evolution of risk management, driven by increasing business complexities, technological advancements, and the changing regulatory environment, has transformed the function from a simple, insurance-focused activity into a strategic, integrated, and dynamic capability of organizations [RCD+22]. As businesses evolve and face new risks, risk management practices are anticipated to continue to mature, offering new ways to navigate the uncertainties of the business world [Mik09].

2.2.1 Integrated Risk Management

IRM is a set of practices, supported by a risk-aware culture and enabling technologies, that improve decision-making and performance through an integrated view of how well an organization manages its unique set of risks [Ser23c]. It has emerged as a critical evolution in risk management, reflecting a shift from fragmented, siloed approaches towards a more holistic, strategic perspective [KPM23; LH03]. At its core, IRM aims to consolidate and coordinate the strategy for managing risks across an organization, ensuring that all forms of risk are considered interconnectedly [RIM18]. A risk in one part of the organization can trigger or escalate risks in other areas. Thus, understanding these risk interrelationships and their cumulative impact is critical for effective risk management [RIM18].

Another factor driving the adoption of IRM is the need for strategic alignment. With traditional risk management approaches, the risk management function often operates in isolation, separate from the strategic decision-making processes. Effective risk management should function as a component of the overall management system, but accomplishing this level of integration with traditional tools is frequently challenging [HT21]. In contrast, IRM aims to align risk management with the organization's strategic objectives, ensuring that risk considerations inform strategy and decision-making [MK15]. A properly integrated risk management framework can deliver analysis and insights that help improve business performance [KPM23].

Moreover, the integrated approach promotes greater efficiency and consistency in risk management processes. By consolidating risk information, organizations can avoid duplication of effort, ensure consistent risk assessment methodologies, and achieve a comprehensive view of the organization's risk profile [BMNR15]. A clear understanding of the overall risk landscape is crucial for organizations to make data-driven decisions. This is, however, hard to achieve if data is dispersed across multiple spreadsheets or documents.

However, implementing IRM has its challenges. It requires a culture of risk awareness across the organization, supported by strong leadership commitment. Moreover, effectively integrating risk management with other business processes requires sophisticated technology systems to handle complex risk data and provide meaningful insights [RIM18].

2.3 Risk Management Tools

Risk management tools are applications or instruments organizations utilize to define their risk management processes, identify and assess risks, and monitor and control the impact of those risks on their business objectives. The complexity and functionality of these tools can vary greatly, from simple, manually updated spreadsheets to fully automated, integrated risk management systems [BMNR15].

With technological advancements, the landscape of risk management tools has evolved significantly [Pri22]. Many software solutions offer a broader range of features and capabilities today [KPM23]. These software solutions can automate many risk management tasks, help track risk changes over time, and alert managers to potential issues. Some even incorporate libraries of common risks, enabling more consistent risk identification and management across an organization [Ser22].

However, it should be noted that advanced risk management tools also bring challenges, such as the need for specialized training, potential high costs, data security issues, and the importance of aligning the tool's use with the organization's unique risk management methodology and objectives [Ave15].

2.3.1 Use of the Microsoft Office Suite for Risk Management

Excel and Word have long been mainstays in risk management due to their simplicity and widespread availability as part of the Microsoft Office Suite. They eliminate the need for specialized training or proprietary software, and because they are standard software in most organizations, they are cost-effective and easy to deploy.

Excel is often employed for its ability to organize and manipulate data. Risk identification, assessment, and tracking are regularly managed through spreadsheets,

where risks are logged along with their characteristics, such as potential impact, likelihood, and assigned mitigation strategies. Using formulas allows for calculations such as risk scoring, while pivot tables and graphs can facilitate rudimentary risk reporting and visualization [PB20]. Excel also allows for risk modeling methods like Monte Carlo simulations, so decision-makers can better understand the range of possible results and their associated probabilities [CW11].

Word is often employed to document the risk management process and related policies and procedures. Detailed descriptions of identified risks, potential impacts, and planned responses can be recorded in Word documents. Additionally, the reporting feature of risk management is often carried out in Word, where findings from risk assessments are compiled into structured reports [HM17].

However, Excel and Word present considerable challenges when applied to risk management at scale. These challenges include difficulty managing and updating large volumes of data, lack of real-time updates and interactivity, and data consistency and integrity [HS16]. They can become especially cumbersome when multiple stakeholders are involved, or risk data needs to be consolidated across different organizational departments or units [BMNR15]. Manually updating risk profiles, recalculating probabilities and impacts, and prioritizing risks often result in outdated data [MK15]. The limitations of Excel and Word underscore the increasing need for more specialized and robust risk management software capable of efficiently handling the complexities of modern risk management.

2.3.2 Software Solutions for Risk Management

Software solutions are emerging as valuable tools for businesses in risk management due to their ability to handle complex and dynamic risk landscapes effectively [Pri22]. These solutions come in many forms, from standalone applications dedicated solely to risk management to integrated modules in more extensive enterprise resource planning systems.

Software tools designed for risk identification and assessment are among the most common. These tools focus on systematically identifying and assessing risks, often utilizing capabilities such as scenario analysis, mapping, and calculating risk metrics [HS16]. However, it is about more than just identifying and assessing risks; monitoring and reporting on these risks are equally critical. Software tools that provide real-time updates and reports on an organization's risk profile are available, featuring user-friendly dashboards that visually represent the risk landscape, making pinpointing areas that need immediate attention easier [BCH05a].

While these software solutions have many advantages, such as improved accuracy, better integration with other business processes, real-time risk monitoring, and

efficient reporting, implementing them is challenging. Organizations may face complexities during the implementation phase, substantial investment requirements, and the potential need to adapt their organizational culture and processes to accommodate the new software [BMNR15; AVS20].

ServiceNow

As organizations strive for more efficient and integrated risk management, software solutions are evolving to meet these needs. ServiceNow's GRC module exemplifies the integrated risk management software solution, where various aspects of risk management, e.g., risk identification and assessment, compliance management, policy and procedure management, and incident management, are combined into a single, integrated platform [Ser23f; Sera]. It offers a comprehensive suite of risk management capabilities within a single platform and supports integration with other organizational processes. ServiceNow's GRC applications help to monitor and identify high-impact risks continuously and to improve risk-based decision-making, thereby reducing reaction time effectively [Ser23a]. By embedding risk management in cross-functional activities, productivity can be increased [Ser23b]. This makes risk management more streamlined and ensures that risk management is an integral part of the organization's overall operations, fostering cross-departmental cooperation and breaking down the traditional silos that can hinder effective risk management [Sera; Serd; Ser23c].

Routine tasks, such as risk assessments and policy compliance evaluations, can be automated, reducing the amount of manual labor involved in these processes [Sera]. In addition to the efficiency this automation provides, it also can increase the accuracy of these processes by reducing the chances of human error [AF20]. The GRC module also provides real-time monitoring and reporting capabilities. These features allow up-to-date overviews of the organization's risk and compliance status to be presented on customizable dashboards. Such real-time insight equips decision-makers with the necessary data to swiftly make informed choices [Sera].

Integration with other business operations is another key aspect of the GRC module. For example, incident reports can be linked to risk assessments, and change management workflows can be tied to policy compliance. Such integrations provide a holistic view of the organization's GRC landscape, encouraging a culture of risk awareness and compliance throughout the enterprise [Sera].

Implementing a GRC module, as with any powerful software solution, comes with challenges. These include substantial investment in resources, time, and training to customize the system to the organization's needs and ensure its successful adoption by the workforce [AVS20].

2.4 Architecture of ServiceNow's GRC Module

The subsequent sections present the architecture of ServiceNow's GRC module, focusing particularly on its central databases and their interlinkages. The architecture enables organizations to remain compliant with regulations while minimizing risks [Ser23c; Ser23d]. An overview of the architecture, with how the different areas are connected, can be seen in Figure 2.2.

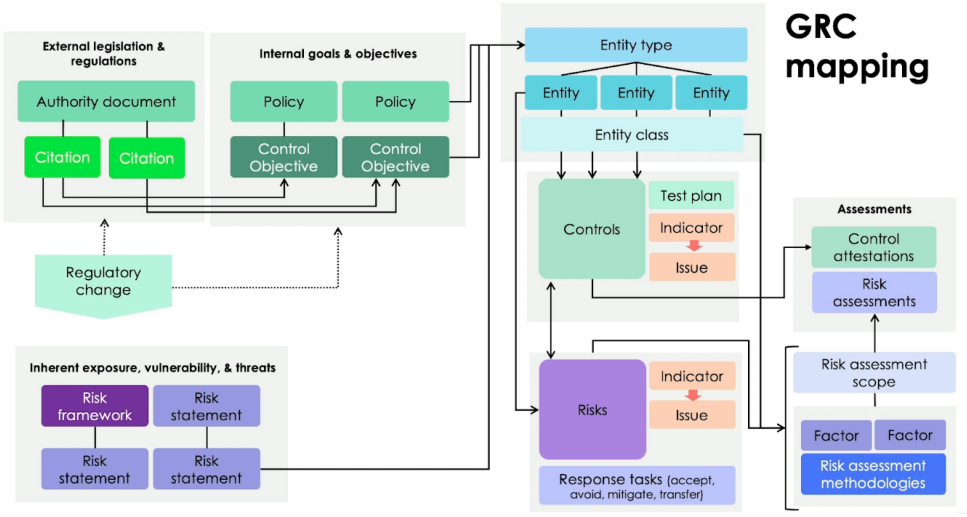


Figure 2.2: Overview of the GRC Architecture in ServiceNow [Ser23d]

2.4.1 Authority Documents and Citations

Organizations must abide by numerous external legislation and regulations depending on their geographic and industry-specific positioning [Ser23e]. Within ServiceNow, these rules and regulations are housed in the Authority Document table at the top level of the compliance framework hierarchy in the ServiceNow instance [Ser23c; Ser23d]. This table is a central hub for regulatory content. Authority Documents encompass requirements set by authoritative bodies, which may include regulations, principles, standards, guidelines, best practices, and procedures. These documents primarily facilitate reporting, follow-up, and audits. The Authority Document table may also store additional content like contractual obligations or international standards. These documents typically incorporate segments called Citations that provide detailed instructions for maintaining compliance and define a section of an Authority Document to which the organization must comply [Ser23d; Ser23c]. Citations are used to report on smaller parts of an Authority Document. A Citation maps to one Authority Document and can be part of hierarchical, parent-child

relationships [Ser23c]. Further, Citations are mapped to and operationalized through Control Objectives, which are elaborated on in the next section. Figure 2.3 illustrates this hierarchy [Ser23c].

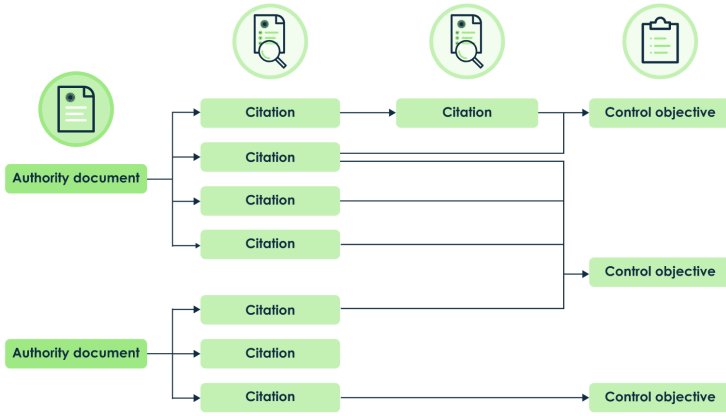


Figure 2.3: Authority Documents, Citations, and Control Objectives Hierarchy in ServiceNow [Ser23c]

2.4.2 Policies, Control Objectives, and Controls

Subsequent in the chain are Policies and Control Objectives, which parallel the structure of Authority Documents and Citations [Ser23c; Ser23d], as shown in Figure 2.3 above. Just as Citations disassemble an Authority Document into smaller, manageable parts, Control Objectives do the same for a Policy [Ser23c]. Policies are pivotal in shaping company culture, covering access control, diversity, security, and sustainability [Ser23c]. Some Policies stem from Citations and facilitate the organization's adherence to necessary regulations.

Control Objective can be considered a standard Control created to comply with one or more internal or external Citations. It is an objective, direction, or standard that guides company interactions and operations [Ser23c]. Control Objectives are often based on Citations, as the Citation wording may be confusing or not specific enough for the organization [Ser23c]. Controls are based on Control Objectives, where a Control is the implementation of a Control Objective for a scoped Entity, which is a unit or object. Entities will be further touched upon in Section 2.4.4. Internal compliance requirements refer to Control Objectives and their corresponding Policies. While Authority Documents and Citations list external obligations for an organization, Policies and Control Objectives record how the organization responds to these requirements [Ser23c; Ser23d]. Furthermore, organizations can measure

compliance with the Control Objectives, allowing for an efficient evaluation of adherence to rules and regulations [Ser23c].

2.4.3 Risk Architecture Overview

The Risk Frameworks and Risk Statements databases follow next, with the former housing a collection of the latter. Risk Statements define the potential impact on the organization if a risk materializes [Ser23b]. It is a general statement about a potential risk that can occur anywhere in the organization, with a defined consequence that can occur if a threat exploits a vulnerability [Ser23c]. Risk Statements serve as a template to generate Risks per Entity. A Risk is the likelihood of a given threat against a potential vulnerability and the resulting impact of that adverse event on the organization, and is the specific occurrence of a Risk Statement against a single Entity [Ser23c]. Controls can be used to mitigate Risks, which involves creating relationships between a Risk and a Control.

Risk Statements can be organized into categorized Risk Frameworks [Ser23c]. To manage numerous Risk Statements more efficiently, organizations can define a Risk Framework to group similar Risk Statements or a hierarchy of Risk Statements into manageable categories. Risk Statements can also be nested in parent-child relationships with or without a Risk Framework. This creates a hierarchy that can be used in reporting and for aggregating Risks so that relevant stakeholders can track and monitor the risk posture at the right level of granularity [Ser23c].

Risk Assessment Methodology

The Risk Assessment Methodology (RAM) defines the process or method for assessing Risks. With configurable RAMs, a company can be flexible in what type of risk assessment is completed across various parts of the business [Ser23c; Ser23a]. A RAM is a unique Risk Assessment template that can be applied to assess a Risk scoped with an Entity or an Object. The RAM defines the types of Assessments conducted, how to determine likelihood and consequence, and how to respond to the Risk Assessment results.

When a RAM template is defined, it can include a single assessment type or any combination of the three available assessment types: Inherent Risk, Control Effectiveness, and Residual Risk [Ser23c; Ser23a]. Inherent Risk is the risk level without Controls or mitigating actions. To determine the overall Inherent Risk score, an organization will assess the impact of the Risk if it occurs and the likelihood of the Risk occurring [Ser23a]. Controls can be preventative, detective, or corrective. In the case of a Risk materializing, Controls can detect its occurrence or mitigate the impact [Ser23c]. Residual Risk is the leftover risk after the implementation of Controls. Generally, the Residual Risk score is calculated based on the effectiveness

of the control(s) and overall inherent risk score [Ser23a]. Figure 2.5 illustrates the three assessment types [Ser23a].

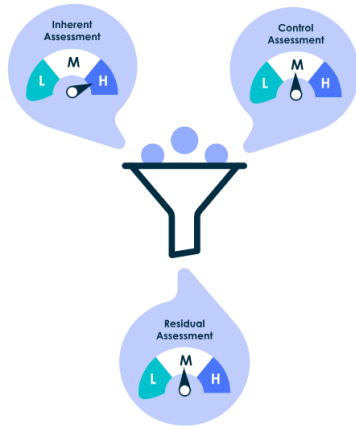


Figure 2.4: Assessment Types in ServiceNow [Ser23a]

2.4.4 Entity Types and Entities

Entity Type and Entity databases represent components like individuals, assets, business processes, and locations that aid in managing controls and risks [Ser23c; Ser23d]. In the context of Risk and Compliance, Entities can be seen as the subjects to assess Risks on and associate Controls with. Entity Types are dynamic categories containing one or more Entities, associated to Policies, Control Objectives, Risk Frameworks, and Risk Statements. Entities can be linked to underlying databases or an existing Configuration Management Database (CMDB). With the utilization of Entities, each database can be measured. This makes the non-compliance of a single database easier to detect, assess, and remediate [Ser23c]. If one database fails, the failed database can be addressed without declaring the whole organization non-compliant [Ser23c]. This also means that remediation efforts are more targeted and efficient for the organization, and streamlines data maintenance across ServiceNow. Applying Entity Types to Risk Statements and Control Objectives generates new records for each entity, a process termed scoping [Ser23a].

Entity scoping is when an organization defines what people, places, or objects, such as processes, vendors, and departments, should be monitored for compliance and included in risk management [Ser23c]. Then, these Entities are mapped to a set of Controls, maintained in the Control Objectives table, and to a set of Risks, maintained in the Risk Statement table. A mature Entity Framework helps an organization create

an integrated risk management program with automatic workflows and informed, data-driven decision-making [Ser23d].

Figure 2.5 illustrates an example of how scoping connects and defines the relationships between Entities and Risk Statements [Ser23c].

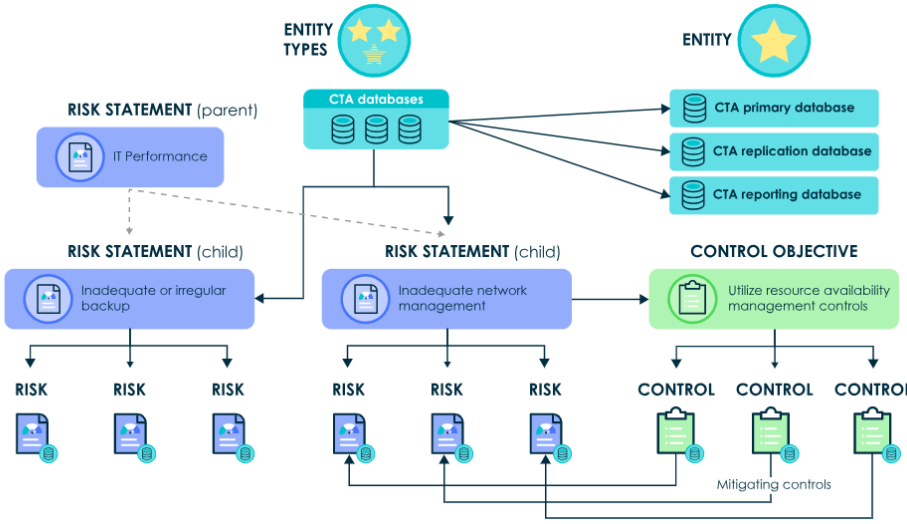


Figure 2.5: Scoping Connections Between Entities and Risk Statements in ServiceNow [Ser23c]

2.4.5 Indicators

Risk and Control owners are primarily responsible for monitoring and evaluating Risks and Controls using tools like Test Plans, Indicators, and Issues [Ser23a; Ser23e]. Test Plans are beneficial during audits, assessing whether a Control is designed effectively and is operating as expected. Indicators help monitor Controls and Risks and gather evidence of performance, while Issues can be linked to a Control or a Risk [Ser23a].

2.5 Risk Libraries

Already in 1994 [Wil94], the centrality of a risk register in risk management infrastructures was noted. It was then suggested that a register could assist in time, cost, and technical analyses, help devise a risk-management plan and prompt decisions on risk transfer. Today, a risk library is foundational to managing and optimizing risk successfully [Hun21].

A standardized risk library is a collection of predefined and standardized risk categories, definitions, and associated risks that are commonly used in a particular industry or organization [Hun21]. It is a systematic approach to consistently identify, assess, and manage risks across various business units, projects, and operations. Risk identification requires a thorough understanding of all the potential obstacles to success, and a risk register can simplify this task by showing at a glance which risks exist, which risks are most worrisome, and how the enterprise should address them [Ris23]. It is an extremely effective tool to enable everyone involved in the project to consciously evaluate and manage the risks as part of the decision-making process [PN02]. It also provides a platform for mitigation actions and decisions to be made in the future by ensuring a greater understanding and acceptance of the visible risks.

The way that risk libraries can instantly elevate the risk performance of an organization represents an exciting new frontier of risk management [Tho21]. Instead of having to spend a lot of time configuring things manually and reworking the entire risk management framework, important risks and controls from trusted libraries can be added to the existing risk taxonomy of the organization. The library provides a common language for risk management professionals and stakeholders to discuss and communicate risks across the organization [PN02]. It also helps ensure that risks are consistently identified and assessed and that appropriate mitigation strategies are implemented.

An organization can internally develop a standardized risk library or purchase it from third-party providers specializing in developing risk libraries for specific industries.

Risk Libraries in ServiceNow

In ServiceNow, a Risk Statement can be considered one entry in the risk library, containing descriptive information about a standard Risk [Ser23d]. Risk statements do not become a Risk unless connected to an Entity. Normally, several Risks stem from one Risk Statement, depending on which and how many Entities are related to the Risk Statement.

Chapter 3
Methodology

This chapter describes the research design and methods for investigating the research questions. Its purpose is to provide readers with a clear comprehension of the steps to investigate the problem and the rationale behind selecting the particular methodology. The study's objectives and the nature of the research questions guide the selection and description of the method.

The thesis uses a qualitative method for data gathering. The study centers around a literature review and an empirical study using interviews. This was chosen because there is much literature on risk management but little research concerning using ServiceNow's GRC module, therefore requiring insight from the real world.

The thesis's process is illustrated in Figure 3.1. Collecting insights and writing has not been linear and often required going back and forth between steps, especially up to writing the discussion.

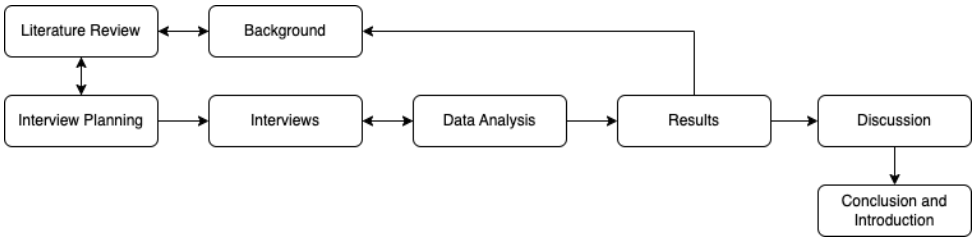


Figure 3.1: Overview of the Thesis Process

3.1 Literature Review

A literature review was first conducted to gather relevant and up-to-date information on ServiceNow, risk management practices, risk reporting, and risk management tools. This encompassed scholarly articles, research papers, industry reports, and other relevant publications related to risk management and the use of ServiceNow. The goal was to gather various sources to understand the topic comprehensively. It is important to note that while the literature review aimed to explore the use of ServiceNow in risk management, it was observed that limited research had been conducted specifically on ServiceNow in this context. However, the relevant literature on risk management practices, tools, and reporting was explored to provide a comprehensive understanding of the field and to draw insights that could be applied to ServiceNow. To gain a thorough understanding of the ServiceNow platform and the GRC module, access to courses from ServiceNow's learning platform NowLearning [Serb] was provided by the supervisor at Sopra Steria. The platform offered valuable resources and insights into the functionalities and applications of ServiceNow for risk management purposes.

Various search engines and databases were utilized to find possibly relevant material, including Google, Google Scholar, and Science Direct. These platforms offered a wealth of academic and industry publications, ensuring a diverse range of sources for analysis. The snowballing technique was employed as an additional method to enhance the comprehensiveness of the review. This involved examining the reference lists of relevant articles and papers to identify additional sources not initially identified through the primary search. To facilitate the search process, keywords such as *Risk Management*, *ServiceNow*, *GRC*, *GRC Tools*, *Risk Management Tools*, *Traditional Risk Management*, *Risk Registers*, *Risk Library*, *Risk Management Efficiency*, *Risk Management Limitations*, and more were used. These keywords helped target literature directly related to the research focus. After gathering and reading the literature, the findings and information were synthesized and organized in the thesis.

Figure 3.2 shows the literature review process. This was not linear, as the entire process was repeated when more literature was needed.

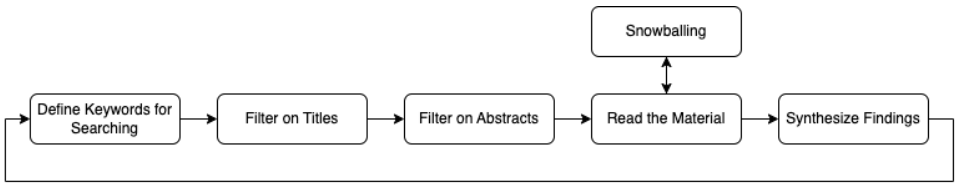


Figure 3.2: Overview of the Literature Review Process

3.2 Interview Process

A qualitative method for gathering data was chosen, as it was considered better suited for the topic than a quantitative method. The topic of the thesis was deemed unsuitable for using, e.g., a survey for data gathering, as it required speaking to experts in the field of risk management who also have experience with ServiceNow. Semi-structured interviews were therefore chosen for gathering the data. Qualitative research gathers insights into people's experiences, whereas quantitative analysis focuses more on numbers and statistics [Cre13]. It is not possible to generalize qualitative data to entire populations, but it can provide valuable insights into specific topics. Therefore it was chosen as the appropriate method for gathering relevant data.

Data Management and Privacy Concerns

To perform interviews that collect personal data, like the interviews did, this must be reported to Sikt, the Norwegian Agency for Shared Services in Education and Research [Nor]. This included making an interview guide and an invitation to participate in the project. The application, approval from Sikt, invitation, and interview guide are attached in Appendices A, B, C, and D.

The interviews were conducted on Microsoft Teams and recorded with the consent of the participants. The recordings were only stored until they had been transcribed, after which they were deleted.

Selection of Interview Objects

The interview participants were chosen with help from the supervisor from Sopra Steria. They were chosen based on their extensive knowledge of risk management and utilizing the ServiceNow platform. They had both been a part of implementing the GRC module in their respective organization and were deemed to have valuable input on the topic. The participants were contacted by e-mail with the invitation to be part of the research project.

Interview Planning

Before conducting the interviews, an interview guide was made, consisting of questions ranging from previous risk management in the organization, use of ServiceNow, and use of a risk library. When making the interview guide, the research questions were kept in mind to get as much insight into the topic as possible. The participants were asked the same questions but with some individual follow-ups.

Performing the Semi-Structured Interviews

Semi-structured interviews have an interview guide to ensure that specific subjects are touched upon but allow follow-up questions when necessary [Cre13]. This type of interview thus provides that the empirical data for the thesis is gathered but opens up for questions not planned in the guide if something deemed relevant emerges during the interview.

At the beginning of each interview, the study was presented to the interviewee before requesting approval to record the interview. The first questions were about the participant's work, background in risk management, and experiences. These questions aimed to gain insight into the interviewee's background and to "warm them up". After the initial questions, the questions in the interview guide were asked. When done with the interview guide and eventual follow-ups, the participants were asked if they had anything they would like to add or any questions. Lastly, the interviewees were thanked for taking the time to participate in the study. The interviews lasted around 45-60 minutes.

3.3 Data Analysis

After the interviews were conducted, they were transcribed and translated into English to make working with the empirical data easier. After these phases, NVivo was used to code the interview answers and categorize the responses. The codes were first split into three categories based on which research question they were related to.

For RQ1 and RQ2, the following codes were used: *Manual/time-consuming work*, *risk landscape*, *process integration/lack of process integration*, *risk culture*, and *risk perception*. Additionally, the categories *Why ServiceNow* and *usage of the GRC module* were used for RQ2. For RQ3, the following codes were used: *Risk perception*, *risk identification*, *usage of a risk library*, and *risk management support*.

After sorting and analyzing the interviews and codes, relevant quotes were extracted. They were then sorted into tables based on the findings they related to. Further, the Results chapter was written. The results and the background material served as the basis for discussing the research questions in the Discussion chapter.

Figure 3.3 shows the data analysis process:

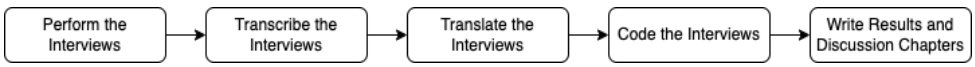


Figure 3.3: Overview of the Data Analysis Process

3.4 Limitations

The limitations of the thesis have already been shed light on in Section 1.2, but the ones most applicable concerning methodology are repeated here.

The sample of interview participants is very limited. When writing a thesis, time is limited, and the interview objects were found at a late stage. If there would have been more time, it would have been preferable to identify more relevant candidates for participating in the semi-structured interviews. A limited sample may not represent the diversity of experiences and perspectives across organizations and industries, and it would have been preferred to include a more diverse sample. Additionally, it could have been interesting to talk to organizations considering implementing ServiceNow and see the expectations of such tools. As stated in Section 1.2, as the participants already have implemented and utilized the GRC module and a risk library in their organizations, their perspectives may be positively biased due to their personal experiences or the organization's investment in these technologies.

The absence of experimental or quantitative data is also a limitation. Quantitative studies or experimental data could provide additional objectivity and the ability to quantify the impact or efficiency of the GRC module and risk library.

Chapter 4
Results

This chapter presents the findings from in-depth interviews with two risk management professionals from distinct organizations who have implemented and utilized ServiceNow's GRC module and a risk library. These interviews aimed to investigate their experiences, how the tools have been implemented within their respective organizations, and how they have impacted their risk management processes.

The findings are based on the participants' narratives, and the chapter's structure is determined by the major themes that arose from the analysis of the interviews. This structured approach comprehends the participants' perspectives on risk management and their organizations' use of the GRC module and a risk library. Each subsection sheds light on specific dimensions. This systematic organization ensures that the results are presented in a logical manner, enabling readers to gain insights into the challenges, benefits, and best practices identified through the interviews.

4.1 Interviewees

The thesis's findings were obtained through in-depth interviews with two professionals working in risk management in their respective organizations. The identities of the interviewees and specific information about their organizations are withheld for confidentiality reasons. Both hold important positions within their respective organizations and participate actively in the risk management process. The participants were chosen based on their extensive knowledge and experience with ServiceNow's GRC module and risk library and their role in managing organizational risk.

The participants' experiences and perspectives are unique to their organizations and contexts and may not represent all ServiceNow's GRC module and risk library consumers. However, their experiences provide valuable insights into the practical considerations of implementing and utilizing these tools and can inform future research and practice.

4.1.1 Participant A

"Participant A" is an experienced risk management professional operating in a large organization. They oversee all delivery teams in terms of risk, monitor the risk landscape for both the teams and the organization as a whole, and conduct risk assessments when introducing new services or making significant changes to existing solutions. Participant A has extensive experience with various risk management tools and methodologies and has been actively involved in implementing ServiceNow's GRC module in their organization.

4.1.2 Participant B

"Participant B" occupies a comparable position in a different industry. Participant B has a comprehensive understanding of risk management, having been exposed to both traditional risk management practices and more contemporary, technology-driven practices. They have worked with risk management in their organization for 9 years. This has covered everything from information security to more general risk management and personnel risk handling. The organization of Participant B has transitioned from traditional risk management methods to the GRC module, enabling them to provide a unique perspective on the transition's effects.

4.2 Results Related to Risk Management

This section presents the key findings related to risk management from the interviews. The focus is on understanding the limitations and challenges associated with traditional risk management practices, and to shed light on existing gaps and inefficiencies in traditional risk management. The findings are based on the analysis of interview data gathered from the participants and offer valuable insights into the practical realities and complexities of risk management processes.

The section is structured into several subsections, each addressing a specific aspect of risk management. The aim is to provide a clear and concise overview of the results, allowing readers to understand the key themes and patterns that emerged from the interviews.

4.2.1 Traditional Risk Management Is Manual and Time-Consuming

The interviews revealed that traditional risk management practices often involved manual and time-consuming processes. The participants described the challenges associated with using manual methods, such as spreadsheets in Excel, for managing and reporting risks. The quotes in Table 4.1 highlight these challenges.

Table 4.1: Quotes Related to Manual and Time-Consuming Risk Management

Interviewee	ID	Quote
Participant A	A-1	"It was challenging to view risks across different areas when we used Excel, as we had to manually scroll through the spreadsheet to get a complete overview."
Participant B	A-2	"When I started, we primarily used Word and Excel, which were time-consuming to maintain. The transition to a more standardized tool made it more dynamic and actively used in decision-making."
Participant B	A-3	"Previously, we had more annual risk assessments, and everything was very manual, which was perceived as challenging."
Participant A	A-4	"Previously, tracking risks involved much manual work and scrolling up and down, which we struggled to find time for."
Participant B	A-5	"One significant challenge was the lack of reusability. We had to manually write everything almost every time, making it difficult to reuse previous work."

These quotes illustrate the manual nature of traditional risk management processes and the associated time-consuming tasks involved in managing and reporting risks. The use of spreadsheets like Excel required participants to manually scroll through extensive data, which hindered the ability to gain a comprehensive overview of risks. Additionally, participants expressed difficulties in reusing previous work, leading to repetitive manual efforts and limited efficiency in managing risks.

Manual Processes Have Limited Scalability

The quotes in Table 4.1 also highlight the limitations associated with limited scalability in traditional risk management processes. Relying on spreadsheets or manual systems to manage risks hampers the ability to handle large amounts of data efficiently. The manual process of scrolling through a spreadsheet to gain a comprehensive overview of risks is time-consuming, cumbersome, and prone to errors. Moreover, the lack of reusability in manual methods makes it challenging to scale the risk management process as the number and complexity of risks increase. This repetitiveness also wastes time and effort, as much of the work cannot be effectively utilized in subsequent analyses or reporting. Adopting more scalable and automated risk management tools and practices can streamline processes, improve data handling capabilities, and enable organizations to manage risks effectively.

4.2.2 With Traditional Risk Management, It Is Demanding to Get an Enterprise-Wide View

The interviews revealed that traditional risk management practices often lack an enterprise-wide view. The participants shared their experiences and challenges related to the limited visibility and aggregation of risk data. The quotes in Table 4.2 highlight their perspectives.

Table 4.2: Quotes Related to Lack of an Enterprise-Wide View

Interviewee	ID	Quote
Participant B	B-1	"It was difficult to see things holistically and aggregate data when we relied on Word and Excel. Everything was performed manually and took an enormous amount of time. Obtaining a holistic view of the risk landscape was very difficult."
Participant B	B-2	"It can be demanding to view things from multiple dimensions, ranging from detailed component-level analysis to overarching organizational governance. Ensuring a methodology and process that works for different purposes and being able to aggregate or align risk management at different levels is a challenge."
Participant A	B-3	"I believe it is easier to overlook things when using an Excel spreadsheet."

These quotes highlight the participants' difficulties in gaining a comprehensive and enterprise-wide view of risks in traditional risk management. The manual nature of processes, such as using Excel and Word, made it time-consuming and challenging to aggregate and analyze risk data. Participants expressed concerns about the limitations of these tools in providing a holistic perspective on risks across different dimensions, areas, and levels within the organization.

The findings suggest that traditional risk management practices often lack the necessary mechanisms to facilitate an enterprise-wide view. The reliance on manual processes and fragmented tools hampers the ability to synthesize risk data from various sources and understand the interrelationships between risks. This limited view may lead to difficulty identifying emerging threats, assessing their impact on strategic objectives, and making informed decisions.

To address this challenge, organizations may need to adopt integrated risk management approaches and technologies that enable the aggregation and visualization of risk data across the enterprise. By leveraging digital platforms and automated

risk management solutions, organizations can enhance their ability to obtain a comprehensive view of risks, identify interdependencies, and make more informed risk management decisions at different organizational levels.

4.2.3 In Traditional Risk Management, Risk Registers Can Be Closed Off and Inaccessible

The interviews revealed that risk registers could be closed off and inaccessible in traditional risk management, leading to security, access control, and information-sharing issues. Participant A shared their experiences and challenges with using Excel as a risk register. The quotes in Table 4.3 highlight their perspectives.

Table 4.3: Quotes Related to Closed Off and Inaccessible Risk Registers

Interviewee	ID	Quote
Participant A	C-1	"Previously, when we used Excel, we had security, access control, and information sharing issues because all the risks were in one Excel spreadsheet. Therefore, that spreadsheet was heavily restricted compared to now [in ServiceNow], where risk registers are easily accessible for everyone."
Participant A	C-2	"When we had [the risks and tasks] in Excel, it was easy for people to forget or lose track of what they were supposed to do, which is understandable. It was difficult to retrieve the information unless you took detailed notes. During risk meetings, you may not have had a complete overview."

These quotes shed light on the challenges of using Excel as a risk register in traditional risk management. Participant A highlighted issues related to restricted access, limited security, and difficulties in information sharing. The centralized nature of an Excel spreadsheet posed challenges in providing easy and secure access to the risk register for all stakeholders.

Participant A also expressed concerns about the Excel-based risk register's lack of visibility and tracking capabilities. The absence of robust task management features made it challenging for individuals to stay informed about their assigned tasks and responsibilities. Additionally, retrieving relevant information from the risk register required detailed note-taking, and during risk meetings, a comprehensive overview was often lacking.

These findings indicate the limitations of closed-off and inaccessible risk registers in traditional risk management. To address these challenges, organizations may

need to adopt modern risk management tools and platforms that provide enhanced accessibility, security, and collaboration features. By utilizing digital solutions, organizations can ensure that risk registers are easily accessible, information is securely shared, and tasks and responsibilities are effectively tracked and managed. This can improve risk awareness, proactive risk mitigation, and more efficient risk management processes.

4.2.4 Traditional Risk Management Often Has a Fragmented Nature

The interviews revealed that a fragmented and inefficient nature can characterize traditional risk management practices. Participant B highlighted using multiple tools, such as Word, Excel, and specialized risk analysis software, leading to a disjointed and non-integrated risk management process. The quote in Table 4.4 exemplifies this aspect.

Table 4.4: Quote Related to Fragmentation In Traditional Risk Management Tools

Interviewee	ID	Quote
Participant B	D-1	"We primarily relied on Word and Excel but had another tool specifically for information security risks. It was a very good tool, but it was only used by those who facilitated and documented risk analyses. For everyone else the process was fragmented, requiring switching between different tools. For example, you would be working on something and then have to switch to a different tool to conduct a risk analysis. Everything was more independent and not interconnected."

This quote illustrates the challenges associated with fragmented risk management practices in traditional approaches. The use of multiple tools for different aspects of risk management, such as documentation, analysis, and specialized risk areas, resulted in a lack of integration and interconnectivity. Participant B described the need to switch between tools, leading to inefficiencies and a disjointed risk management process.

The finding suggests that the fragmented nature of traditional risk management can hinder effective risk assessment, analysis, and decision-making. It can result in information silos, limited collaboration, and difficulty aggregating and synthesizing risk-related data and insights. The lack of integration between tools and processes can impact the organization's ability to gain a comprehensive and cohesive understanding of its risk landscape.

4.2.5 A Robust Risk Culture is Essential for Efficient Risk Management

The interviews highlighted the importance of fostering a robust risk culture to ensure efficient risk management practices. The participants emphasized the need for cultivating an organizational mindset that values and integrates risk management into decision-making processes. The quotes in Table 4.5 illustrate the significance of a strong risk culture.

Table 4.5: Quotes Related to Risk Culture

Interviewee	ID	Quote
Participant B	E-1	"We have spent a lot of time building a culture around emphasizing that risk management is not just about reducing and closing risks. In addition to working on actions, it's also about accepting risks and making that visible. This was necessary because we noticed several lingering risks without much handling."
Participant A	E-2	"Making employees aware of what risk entails is difficult. We are a fairly dynamic organization with frequent personnel turnover. Even though I work with risk daily and have monthly meetings with others, it doesn't mean they have the same understanding of risk as I do. Establishing a clear understanding of our risk appetite and the acceptance criteria we should apply to risks is difficult."
Participant B	E-3	"We have found that working on culture building and engagement has been crucial in actively getting people to use risk management. We have implemented various measures to avoid the perception that [risk management] is done just because it has to be done and instead emphasize its practical usage in daily operations. We worked on getting people to understand the value of risk management and to include risk assessments in decision notes for governing bodies, ensuring its practical utilization."

These quotes emphasize the significance of developing a risk-aware culture within organizations. Participants highlighted the need to create awareness and understanding of risk management principles and practices among employees at all levels. This includes integrating risk assessments into decision-making processes, promoting active engagement with risks beyond risk reduction, and ensuring clear risk appetite and acceptance criteria communication. The dynamic nature of organizations and personnel turnover can make it challenging to maintain consistent awareness and com-

prehension of risk-related concepts. Establishing clear and meaningful risk appetite and acceptance criteria requires a comprehensive understanding of the organization's goals, values, and risk tolerance.

A robust risk culture is essential for effective risk management as it enables proactive risk identification, assessment, and mitigation. It fosters a shared understanding and commitment to managing risks, encourages accountability, and facilitates timely decision-making. By embedding risk management into the organizational culture, organizations can enhance risk awareness, promote risk-informed actions, and improve overall risk management effectiveness.

4.3 Results Related to Implementation of ServiceNow's GRC Module

This section presents the findings related to implementing ServiceNow's GRC module, as revealed through the interviews. The focus is on understanding the experiences and insights of the participants regarding adopting ServiceNow's GRC module within their organizations. By examining their perspectives, this section sheds light on the benefits, challenges, and outcomes of implementing the risk management solution.

The findings presented here are based on the interview data, providing firsthand accounts from the participants with direct experience implementing ServiceNow's GRC module. By examining the experiences and perspectives of the participants, this section contributes to the body of knowledge surrounding the implementation of ServiceNow's GRC module. The insights gathered here can inform organizations considering or currently undergoing a similar implementation, offering considerations for optimizing the use of this technology in their risk management practices.

4.3.1 Companies Choose ServiceNow for Risk Management Because They Use It Elsewhere in the Organization

The decision of companies to opt for ServiceNow's GRC module for risk management is driven by the widespread utilization of the platform within other areas of the organization. The quotes in Table 4.6 highlight the key reasons behind choosing ServiceNow.

Table 4.6: Quotes Related to Why Companies Choose ServiceNow

Interviewee	ID	Quote
Participant A	F-1	"The main reason ServiceNow was a very natural choice for us is because it is the ticketing system we use in [a part of the organization] regularly. It is a system that the customer teams, in particular, were already familiar with. It was a natural choice for us because ServiceNow had already been adopted in other areas."
Participant B	F-2	"The main reason [to choose to implement ServiceNow's GRC module for risk management] was that others already used it in the organization. It was important for us to build on existing data and integrate risk management into daily operations. The ability to reuse the platform and its data, particularly the CMDB (Configuration Management Database) functionality, is unique and highly beneficial."
Participant A	F-3	"I feel that people have found it beneficial to use ServiceNow because we were already using it in other areas. Additionally, many of our customers already have experience with ServiceNow, especially the larger ones, which makes it convenient to use externally."
Participant B	F-4	"I wouldn't necessarily claim that ServiceNow is superior to other GRC tools. It works well for us because the rest of the organization uses it, and we have embedded risk management into their processes. If we didn't have that level of integration, other tools like BWise or Archer would be just as good. We also use BWise for non-IT risks today."

These quotes emphasize the advantage of selecting ServiceNow's GRC module for risk management based on its existing adoption and integration within the organization. Participants highlight employees' familiarity with the platform, particularly in areas where ServiceNow is already being utilized. Leveraging the platform's existing adoption provides a seamless transition and facilitates the integration of risk management practices into daily operations. By building upon existing data and utilizing the CMDB functionality, organizations can benefit from the reuse of information, streamlining processes, and enhancing the overall efficiency of risk management. Moreover, the familiarity of ServiceNow among customers offers additional convenience and compatibility, fostering collaborative risk management efforts.

It is worth noting the acknowledgment that ServiceNow is not inherently superior to other GRC tools. However, the level of integration within the organization and embedding risk management into existing processes contribute to ServiceNow's effectiveness. Participant B suggests that other tools could be equally suitable if they

were similarly integrated.

The findings underscore the strategic advantage of choosing ServiceNow's GRC module for risk management, driven by the organization's preexisting usage of the platform and the successful embedding of risk management practices. By capitalizing on integration, familiarity, and process alignment, companies can leverage ServiceNow to enhance collaboration, streamline risk management workflows, and achieve greater risk management efficiency.

4.3.2 Implementing ServiceNow's GRC Module Takes Thorough Planning

Implementing ServiceNow's GRC module requires careful planning and consideration, as highlighted by the insights shared by the participants. The quotes in Table 4.7 exemplify the significance of thorough preparation and strategy in successfully adopting and integrating the GRC module within an organization.

Table 4.7: Quotes Related to Planning the Implementation of the GRC Module

Interviewee	ID	Quote
Participant A	G-1	"It is crucial to thoroughly understand and consider how to use [the GRC module] and where to begin. We quickly realized that implementing it couldn't be accomplished in one go. There is a lot to learn, many choices to make, and various considerations regarding methodology. The experience taught us that it is crucial to do thorough research in advance to create a solid plan for its usage and the roll-out within the organization."
Participant B	G-2	"We have had a very clear strategy all along to work on both the technology which the GRC module provides, and on the people who will use it and the organization as a whole. It has been a collaboration where updating our governing documents, requirements, and processes has been necessary."

The quotes emphasize the importance of undertaking thorough research, establishing clear strategies, and successfully collaborating to implement ServiceNow's GRC module. Implementing the module involves understanding its functionalities and considering the organization's needs, existing processes, and governing documents. Additionally, effective communication and user guidance are vital in facilitating a smooth transition and maximizing the benefits of the GRC module within the organization. The findings underscore the significance of thorough planning, stakeholder

engagement, and effective change management practices to optimize the implementation process and realize the full potential of ServiceNow's GRC module in supporting risk management endeavors.

Participant A emphasizes the importance of understanding the GRC module's capabilities and functionalities and the need for careful deliberation on the implementation approach. It highlights the necessity of conducting extensive research and creating a well-defined plan that aligns with the organization's objectives and requirements.

Participant B underscores the holistic nature of the implementation process, encompassing not only the technical aspects but also the human and organizational factors. They emphasize the importance of developing a comprehensive strategy that includes updating governing documents, revising requirements, and refining processes to align with the GRC module's capabilities and support its effective utilization. Implementing changes can be complex and time-consuming. The quotes emphasize the importance of clear communication, thorough documentation, and comprehensive user guidance to facilitate a smooth transition and effectively utilize the module's features.

4.3.3 Customization of ServiceNow's GRC Module Can Result in Technical Challenges

Customizing ServiceNow's GRC module can present technical challenges, as highlighted by the insights shared by the participants. The quotes in Table 4.8 exemplify the difficulties encountered during the customization process and the potential impact on implementation and future updates.

These quotes shed light on technical challenges organizations may face when customizing ServiceNow's GRC module. Customizations can introduce complexities, potentially impacting the implementation timeline and user experience. Participants emphasized the importance of thorough research and consideration before making customizations and finding a balance between standard functionality and tailored adjustments.

Participant A highlighted the challenges when attempting to customize and simplify the GRC module and align it with the organization's needs. They acknowledged encountering technical issues during the customization process, primarily due to making changes and modifications. The technical challenges experienced when aligning the GRC module with their organization's needs resulted in delays and adjustments, affecting the initial introduction and user experience. The customization process was essential to tailor the tool to their organization's requirements. Still, the participant

expressed a desire for more thorough consideration and research on the impact of customizations before implementing them.

Participant B highlighted the potential complexities and challenges of customizing the GRC module. They acknowledged that customization may require additional adjustments during future updates and deployments, which can be time-consuming. While striving to utilize the out-of-the-box and standard functionality, the participant recognized the necessity of customization in certain areas. The quote emphasizes balancing standard functionality and customizations to achieve the desired outcomes without introducing unnecessary complexities.

These quotes underscore the technical challenges of customizing ServiceNow's GRC module. They emphasize the need for thorough research, planning, and consideration of the implications of customizations on the tool's functionality, updates, and overall user experience. The experiences highlight the importance of careful evaluation and balancing customization needs with the advantages of standardized functionality.

Table 4.8: Quotes Related to Customization Challenges

Interviewee	**ID**	**Quote**
Participant A	H-1	"We encountered some technical issues initially, mainly due to making changes or modifications. We would have considered these aspects more thoroughly before implementation if given the opportunity. If we were to start over, we would have researched how various customizations affect the tool more."
Participant A	H-2	"The challenges associated with our customizations resulted in things taking more time. People may not have received the introduction they expected initially because we had to address technical issues first. This was mainly because we needed to customize it to fit our organization."
Participant B	H-3	"When making various customizations, it can increase complexity and potential challenges during future updates and deployments. It may require going back and making adjustments when new features are introduced. We try to stick to the out-of-the-box and standard functionality as much as possible, but we acknowledge that in some areas, customization is necessary. It's important to balance standard functionality and customizations to achieve the desired results without creating unnecessary complexity."

4.3.4 Implementing ServiceNow's GRC Module Requires Good Employee Training

Implementing ServiceNow's GRC module requires a strong focus on employee training, as highlighted by the participants. The quotes in Table 4.9 emphasize the importance of comprehensive training initiatives.

Table 4.9: Quotes Related to Employee Training

Interviewee	ID	Quote
Participant A	I-1	"Having a solid training plan before rolling it out is crucial. We didn't have enough resources dedicated solely to training, making it challenging to educate the entire organization. In hindsight, I would have researched available training materials that could have been sent out in advance, allowing familiarization before the implementation."
Participant A	I-2	"If our approach had been more systematic, we would have rolled it out to one team at a time. That way, you can train and educate one part of the organization at a time, rather than trying to tackle everything at once. I believe such an approach is important."
Participant B	I-3	"We have conducted many training sessions and spent significant time creating training materials. Initially, we created instructional videos, held open-house sessions, and established a community where we presented information. We now use a combination of risk facilitation and standard training videos. We aim for the organization to be as self-sufficient as possible, but with the complexity of the tool, it can be challenging. We try to utilize various platforms and channels for training and invest time in forums where employees can provide feedback."
Participant A	I-4	"The most significant challenge has been ensuring that people understand how it works and can find information. This can be addressed through effective communication and training materials. If we were to 'roll back' the project and start over, we would have initiated training much earlier and provided ample information to individuals before the implementation."
Participant B	I-5	"Implementing any changes generally takes significant time. For example, we have been a bit slow in transitioning to the new Workspace interface. It works perfectly fine, but we need to explain, write documentation, provide user guidance, and effectively communicate the upcoming changes."

The participants highlighted the critical role of employee training in successfully implementing ServiceNow's GRC module. A solid training plan is essential to familiarize employees with the functionalities and usage of the tool, ensuring that they can effectively navigate and utilize it in their risk management activities. Comprehensive training initiatives should include a variety of methods, such as instructional videos, open-house sessions, and dedicated communication channels, to accommodate different learning styles and facilitate widespread understanding. Creating a community can enhance employee engagement and knowledge sharing.

The complexity of the tool may present challenges in training efforts, requiring continuous improvement and adaptation of training materials. Integrating feedback mechanisms allows for ongoing refinement of training approaches and ensures employees feel empowered to utilize the GRC module effectively. By initiating training early in the implementation process, individuals get time to familiarize themselves with the tool and its functionalities. Effective communication and training materials are key to addressing tool comprehension and information retrieval challenges within the GRC module. By prioritizing employee training and investing in comprehensive and continuous learning initiatives, organizations can maximize the benefits of ServiceNow's GRC module, ensure user proficiency, and enable employees to leverage the tool's capabilities to support their risk management endeavors.

4.4 Results Related to the Use of ServiceNow's GRC Module

This section presents the findings related to using the GRC module for risk management, as revealed through the interviews. The focus is on understanding the experiences, benefits, and challenges the participants encounter when utilizing it within their organizations. By examining their perspectives, this section sheds light on the practical implications and outcomes of using a technology-driven solution for managing risks.

The findings presented in this section are derived from the analysis of interview data, and these insights offer information on the technology's effectiveness, efficiency, and impact in managing risks across different organizational contexts. By examining the experiences and perspectives of the participants, this section contributes to the body of knowledge surrounding the use of ServiceNow's GRC module for risk management. The insights gathered here can inform organizations considering the adoption of this technology, providing valuable information on its potential benefits and challenges. Additionally, these findings can assist organizations already using it in optimizing its utilization and identifying areas for improvement in their risk management practices.

4.4.1 The GRC Module Provides a Better View of the Risk Landscape

Implementing ServiceNow's GRC module has proven instrumental in enabling organizations to obtain a comprehensive and improved view of their risk landscape. The quotes in Table 4.10 shed light on the significance of the GRC module in enhancing risk visibility.

Table 4.10: Quotes Related to Risk Landscape Overview

Interviewee	ID	Quote
Participant B	J-1	"I believe that ServiceNow can help provide a better view of the risk landscape, but it heavily relies on good data quality and structure. ServiceNow can assist when you have a solid foundation with accurate and reliable information about risks and resources. However, this is also a significant job."
Participant A	J-2	"I think the implementation of the GRC module has contributed to shedding light on areas and providing a better understanding of the risk landscape. It may reveal that certain areas previously considered low-risk have many associated risks. I believe that the GRC module helps provide a more realistic picture of the actual risk situation and assists individuals in identifying risks because it offers different categories to associate risks with, making it easier to recognize and navigate within the system. There is no doubt that it provides us with a risk picture."

These quotes underscore the GRC module's ability to enhance organizations' visibility into their risk landscapes. The effectiveness of the module relies on the availability of good data quality and a well-structured foundation of risk and resource information. The module can significantly improve organizations' understanding of risk profiles when these prerequisites are met.

Implementing the GRC module assists in revealing hidden risks and facilitates a more realistic depiction of the risk situation by uncovering potential risks in previously perceived low-risk areas. Participant A mentioned resources as an example in the interview. Resource management might be seen as part of daily operations. If suddenly you have 30 risks related to personnel, that's a significant number, which may warrant efforts to mitigate them regardless. By offering different categories for risk association, the module streamlines the identification process, making it easier for individuals to navigate and recognize risks within the system.

The GRC module enables organizations to gain a more comprehensive and accurate picture of their risk landscape and identify and evaluate risks more effectively, fostering a proactive approach to risk mitigation. By leveraging the features and functionalities, organizations can enhance risk visibility, strengthen decision-making processes, and allocate resources efficiently to address critical areas of vulnerability. The subsequent sections will delve into specific areas of how it can help enhance the overview of the risk landscape.

The GRC Module Enables Process Integration

An important part highlighted by the participants in obtaining a comprehensive overview of the risk landscape was the possibility of seamlessly integrating risk management into their existing processes. The quotes in Table 4.11 stress this.

Table 4.11: Quotes Related to Process Integration

Interviewee	ID	Quote
Participant A	K-1	"If a change, request, or incident is relevant to a risk, the tool has a seamless connection. That kind of tracking is something we wanted to have concerning different types of risks."
Participant B	K-2	"By directly connecting to processes and data, we can uncover deviations or other factors that may have gone unnoticed previously. It has helped in capturing deviations that we wouldn't have found otherwise. We work more proactively after implementing ServiceNow; however, it still involves manual effort. We need to identify things through dashboards, anomalies, or changes and then reach out to address them. Still, with data connections and automated Indicators, it becomes easier to see that changes are happening."
Participant B	K-3	"Since we use ServiceNow for several other processes, we can incorporate Indicators related to the risks we have identified. This allows us to detect changes in the data, leading to changes in the risk landscape. This was impossible when we relied on Word and Excel."

These quotes emphasize the advantages of process integration provided by the GRC module. Organizations can establish a seamless connection between risk-related activities and other operational processes within the tool. This integration allows comprehensive tracking, ensuring that risk-related changes, requests, or incidents are efficiently linked and monitored. By facilitating this level of connectivity, the

GRC module enables organizations to streamline their risk management efforts and ensures a more holistic approach to risk assessment and mitigation.

The quotes shed light on the fact that although the GRC module in ServiceNow has streamlined the risk management process, manual work is still needed. Identifying risks and anomalies through dashboards or changes requires active involvement and decision-making by individuals. This highlights that the module serves as a tool to support risk management, but it does not eliminate the need for human intervention and judgment.

Furthermore, integrating processes and data within the GRC module enables organizations to uncover deviations or factors that may have gone unnoticed. Combining data-driven insights, qualitative inputs, and quantitative analysis in risk assessments enhances the organization's ability to identify and address potential risks and changes in the risk landscape. This comprehensive approach to risk management contributes to better decision-making and enables organizations to manage and mitigate risks proactively, ultimately protecting their objectives and supporting strategic initiatives.

The GRC Module Makes Risk Management More Ingrained In Daily Operations

Another important aspect highlighted by the participants is that risk management is more ingrained in daily operations after implementing the GRC module, enabling a better overview and insight into the risk landscape. The quotes in Table 4.12 emphasize this.

The quotes underscore how the GRC module has transformed risk management into a more integrated and seamless part of daily operations. By leveraging data connections and automated indicators, individuals can easily detect critical events, changes, or vulnerabilities that impact their risk landscape. This streamlined approach eliminates the need for additional effort and makes risk management a natural and lightweight component of their everyday work. As a result, risk management practices are more actively utilized and incorporated into employees' daily routines.

Integrating risk management into various processes through standardized data fields and centralized approaches has further enhanced its visibility and integration within daily operations. Risk management becomes a structured and visible part of the organizational landscape, ensuring it receives attention and focus. The easy accessibility to insights and the ability to actively work with the system contributes to more effective risk management practices, enabling organizations to proactively address risks, evaluate the success of risk mitigation measures, and make informed decisions to ensure business resilience.

Table 4.12: Quotes Related to Daily Risk Management Operation

Interviewee	ID	Quote
Participant B	L-1	"By enabling individuals to detect critical events, changes, or vulnerabilities that impact their risk landscape without much effort due to data connections and Indicators, it becomes a more natural part of their everyday work, and people use risk management in practice. It makes it more lightweight and connected to their daily routine."
Participant B	L-2	"[The GRC module] has helped establish a more structured and centralized approach. The integration of risk management into various processes has made risk management a more visible part of daily operations. By using Indicators, we can focus on the relevant risk that has changed. It eliminates the need for large, cumbersome annual analyses and promotes more dynamic risk management where things evolve and are addressed in daily operations."
Participant A	L-3	"Risk management is easier now than before. The GRC module makes it easy for people to have an overview of their tasks, simplifying actively engaging with the actions that must be implemented and executed. You can assess whether the measures are achieving their intended purpose regarding risk assessment and ensuring that we follow through with tasks. All insights are easily accessible, allowing you to actively work with it, contributing to more effective management."
Participant A	L-4	"Previously, I would enter meetings with a status update once a month. Now, people enter multiple updates between meetings. Risk registers and similar tools are accessible to everyone who needs to use and actively engage with them. This solves a challenge we faced with Excel. One of our goals in transitioning to ServiceNow was to enable individuals to be more actively involved and have a more conscious approach to their risks."

With the module's features and functionalities, individuals can gain a comprehensive overview of their tasks and responsibilities. The module simplifies the process of actively engaging with the necessary actions and tasks to be implemented and executed. This streamlined approach enables individuals to better understand their specific roles in addressing risks and ensures that risk-related tasks are managed and monitored. In contrast to the limitations of Excel, the GRC module ensures that risk-related information and tools are readily available to everyone who needs to

use and actively engage with them. With the module's implementation, individuals can now enter multiple updates between meetings, enabling real-time tracking and monitoring of risks.

The GRC Module Provides a Dynamic and Ongoing Risk Overview

The participants also highlighted the enhanced risk overview provided by a more dynamic and ongoing risk nature. The module's dashboard offers a live view of risks and issues, enabling individuals to easily identify different types of actions and track their respective responsibilities. This real-time visibility enhances the organization's ability to stay informed and proactively manage risks. This is stressed in the quotes in Table 4.13.

Table 4.13: Quotes Related to a Dynamic Risk Overview

Interviewee	ID	Quote
Participant A	M-1	"The dashboard provides a more live view than before. We have better visibility of risks versus issues, and it is much easier for individuals to find different types of actions and identify the tasks or actions they are responsible for."
Participant B	M-2	"Previously, if you closed a risk, it would disappear. In ServiceNow, even if you accept the risk and have reduced it to a low level, you still keep it in monitoring because things can change in relation to your processes or data. This significantly strengthens risk management and provides a living picture."
Participant B	M-3	"When I look at the other areas of risk management that do not involve IT in the organization, we don't have the same level of dynamism. It's more of the traditional way of working where you conduct a risk assessment, close it, and only reopen it when necessary. With the GRC module, it is integrated with the rest of the organization and perceived as more relevant and ongoing."

A significant improvement brought by the GRC module is the retention of closed risks in the monitoring phase. Unlike previous approaches where closed risks were considered resolved and no longer monitored, ServiceNow maintains their visibility. This practice recognizes that risks can change over time, and even low-level risks may require ongoing monitoring to ensure continued risk mitigation and adaptability. This shift enhances risk management practices by providing a living picture of the risk landscape and facilitating a more proactive approach to risk monitoring and mitigation.

The GRC Module Enables Effective Risk Monitoring Over Time

The implementation of ServiceNow's GRC module has significantly improved risk monitoring capabilities over time, as evidenced by the following quotes in Table 4.14.

Table 4.14: Quotes Related to Risk Monitoring Over Time

Interviewee	ID	Quote
Participant B	N-1	"For us, the Indicators feature has been invaluable for monitoring risk over time, and it is the function we use the most. It has been instrumental in capturing changes in different systems and processes. Indicators are a significant strength of ServiceNow, and an area we will continue to focus on more and more."
Participant A	N-2	"There are trend charts available for both risks and issues, enabling us to track them over longer periods. In this regard, the GRC module has excellent capabilities to provide us with insights into the risks we have reduced and the risks we need to address in the future. We can also track the risks associated with different categories over time. This enables us to monitor trends regarding what we identify, and I believe there are many opportunities to pick up early signals."
Participant A	N-3	"I think the GRC module will provide us with completely different capabilities regarding historical tracking. When we used Excel, we could close cases, but they were not linked to anything specific – they were just individual rows in a spreadsheet without any direct connection. With the GRC module, we can link cases to Risk Statements, log assessments, and track actions. This will provide us with much more insight over time, something we didn't have the opportunity to do before."

These quotes highlight the enhanced risk monitoring capabilities provided by the GRC module, particularly in terms of tracking risks over time. The Indicators feature is a valuable tool for capturing changes in systems and processes, allowing for comprehensive risk monitoring and management. Participants also emphasize the availability of trend charts, enabling tracking risks and issues over longer periods. This functionality empowers organizations to gain insights into risk reduction progress and identify emerging risks, enhancing their ability to make informed decisions and take timely actions.

The GRC module's historical tracking capabilities significantly improve over

traditional methods like Excel. The module links cases, risk statements, assessments, and actions, providing a comprehensive and interconnected view of risk management activities. This enables organizations to gain deeper insights into risk trends, identify patterns, and monitor the effectiveness of risk mitigation strategies over time. By facilitating historical tracking and analysis, the GRC module enhances organizations' understanding of risk dynamics and supports proactive risk management.

The GRC Module Enhances Risk Reporting

The implementation of ServiceNow's GRC module has enhanced risk reporting capabilities, as highlighted by the quotes in table 4.15.

Table 4.15: Quotes Related to Risk Reporting

Interviewee	ID	Quote
Participant A	O-1	"Individuals can easily access and extract an overview or report on their own. Reports can be easily shared with customers, who also have their own overview in their dashboards. When reporting, getting a comprehensive view and extracting relevant data is easier. ServiceNow is much better suited for presenting the data clearly and concisely than Excel, with great potential for data visualization. It is also much easier to find good and relevant data, such as identifying risks that impact multiple deliveries or risks with high consequences in a specific area."
Participant B	O-2	"We have several ways of communicating the results. The risk assessments become part of the risk profile associated with the asset or process and are aggregated into various views, e.g., by section and division levels or by dashboard. Graphs and trend reports can be created and generated in seconds. We also get to present things more continuously and dynamically on a level which would have never been achieved in Word and Excel."

These quotes emphasize the enhanced risk reporting capabilities facilitated by the GRC module. The module enables individuals to easily access and extract comprehensive overviews and reports, empowering efficient communication with customers, management, and other stakeholders. Compared to traditional tools like Excel, ServiceNow excels in presenting data clearly, concisely, and visually appealingly. The module's robust data visualization capabilities and intuitive dashboards enable effective data exploration, identification of risks impacting multiple deliveries and identification of risks with high consequences in specific areas.

4.4.2 The GRC Module May Be Perceived As Complex

The implementation of ServiceNow's GRC module presents both opportunities and challenges, as expressed by Participant A. The quote in Table 4.16 sheds light on the complexity associated with the GRC module.

Table 4.16: Quote Related to Complexity

Interviewee	ID	Quote
Participant A	P-1	"Although there have been some challenges related to the complexity, especially for those who don't work with it daily, there is a general enthusiasm among people. They are eager to learn and utilize the tool. They recognize the opportunities various dashboards offer and the overview they can provide if they learn to use the Workspace feature. Even though they acknowledge there is a lot to explore within the tool, I have observed a positive attitude among individuals. While the GRC module may initially seem large and somewhat overwhelming when learning it, it becomes clear and beneficial once you become more familiar with its functioning."

The quote highlights that the GRC module can be perceived as complex, particularly for individuals not regularly engaging with it. The initial learning curve and the extensive functionality of the tool may seem overwhelming. However, the quote also reflects a positive attitude among individuals who recognize the opportunities presented by the GRC module. There is a sense of enthusiasm to learn and utilize the tool, driven by its potential benefits, such as comprehensive dashboards and the Workspace feature for improved overview and functionality.

The findings indicate that while the GRC module may present complexity and require dedicated effort for understanding and proficiency, individuals who invest time and effort to familiarize themselves with its functioning can overcome the initial challenges. With increasing familiarity, the GRC module becomes clearer and its benefits more apparent, leading to positive perception and utilization.

The complexity of the GRC module underscores the importance of providing adequate training, support, and ongoing learning opportunities to empower users and maximize the tool's benefits. Organizations can promote a positive learning environment and encourage individuals to explore and embrace the functionalities of the GRC module, ultimately leveraging its capabilities for more effective risk management and decision-making.

4.4.3 The GRC Module Should Be Simplified

The participants' insights highlighted the wish to streamline and simplify the GRC module to enhance its usability and user experience. The quotes in Table 4.17 highlight the wish for simplification.

Table 4.17: Quotes Related to Simplifying the GRC Module

Interviewee	ID	Quote
Participant A	Q-1	"If I were to change something about the GRC module, I would probably streamline the functionality and remove any features we don't use. We have noticed about 4-5 highly relevant features for people to use, while others could be eliminated from the menu. So, if I were to make any changes, I would simplify it beyond what we have already done."
Participant B	Q-2	"I would prefer a much simpler user interface. The interface requires a lot of clicking to perform simple tasks. We have managed to streamline some processes to reduce the number of clicks, but there is still room for improvement. Previously, it would take 20-30 clicks to get one risk through, and if there were associated actions, it would require even more clicks. So, having a simpler user interface would be a significant improvement."

The quotes emphasize the importance of simplifying the GRC module to optimize user experience and efficiency. Participant A expressed the need to streamline the module's functionality by removing unnecessary features not utilized by the organization. By focusing on the most relevant and essential features, organizations can improve usability and ensure users can navigate the system more efficiently.

Participant B highlighted the significance of a simpler user interface. They expressed concerns about the current interface, which requires excessive clicking to perform simple tasks. Simplifying the interface by reducing the number of clicks and enhancing user-friendly design elements can significantly improve the user experience, reducing frustration and increasing productivity. Streamlining functionality and improving the user interface can create a more intuitive and efficient platform for risk management activities. Simplification facilitates ease of use, reduces complexity, and enables users to focus on essential tasks, ultimately improving overall user satisfaction and the effectiveness of risk management processes.

The GRC Module Still Requires Manual Work

The implementation of ServiceNow's GRC module has brought improvements to the risk management process, but it still requires a certain level of manual effort, as both indicated by quote Q-2 and the following quotes in Table 4.18.

Table 4.18: Quotes Related to Manual Work Within the GRC Module

Interviewee	ID	Quote
Participant B	R-1	"There is a lot of data entry and numerous fields in ServiceNow, which means that not everyone is equally proficient in documenting all the required information."
Participant A	R-2	"The GRC module has a lot of mandatory fields that must be filled out. For example, you cannot enter an incomplete risk without completing all necessary assessments."

These quotes shed light on the fact that although the GRC module in ServiceNow has streamlined the risk management process, manual work is still needed. The data entry aspect of the GRC module presents a challenge. With numerous fields to be completed, individuals must be proficient in accurately documenting the required information. This requirement may pose a learning curve for some users and may necessitate additional training and support to ensure consistent and accurate data entry. Moreover, the presence of mandatory fields within the GRC module reinforces the need for thoroughness and completeness in risk assessments. While this requirement ensures that all necessary information is captured, it adds to the manual workload of utilizing the module.

4.4.4 The Use of ServiceNow Impacts Competency Needs

ServiceNow has brought about notable changes in organizational competency requirements and needs, as Participant B highlighted. The quotes in Table 4.19 shed light on the impact of ServiceNow on competency requirements.

Table 4.19: Quotes Related to Competency Needs

Interviewee	ID	Quote
Participant B	S-1	"There has been a shift from being facilitators with expertise in the field, focused on processes and methodology, to a greater emphasis on the tool and data. Having extensive risk management knowledge is no longer necessary, which has also changed the internal skill requirements. This demonstrates how implementing technological solutions can impact an organization's competence requirements and role understanding. Our team has two individuals dedicated solely to tool development and data, working exclusively within the tool, and we could easily use a couple more."
Participant B	S-2	"We have monthly sprints for further development or improvements that we undertake. Some of the changes require developers, for which we create user stories. Additionally, there are low-code elements and tasks that we handle ourselves."

These quotes emphasize the impact of ServiceNow on the competencies and roles within organizations. The implementation of ServiceNow has shifted the focus from extensive risk management knowledge to proficiency in utilizing the tool and managing data. It has transformed the role of risk management professionals, requiring them to adapt to technological advancements and leverage ServiceNow's capabilities effectively. As highlighted by Participant B, the utilization of ServiceNow may necessitate dedicated individuals for tool development and data management, indicating a need for specialized skills in these areas. The implementation of ServiceNow also introduces agile practices, such as monthly sprints and user stories, which further impact the competencies required within the organization.

This insight demonstrates that the utilization of ServiceNow as a technological solution in risk management has led to a reconfiguration of competency requirements and skill sets. Organizations are shifting their focus towards developing expertise in utilizing the tool, managing data, and leveraging low-code elements. This highlights the dynamic nature of technological implementations and the importance of continually evolving competencies to maximize the benefits of such solutions.

4.5 Results Related to the Use of a Risk Library

This section presents the findings related to the use of a risk library to enhance risk management, as uncovered through the interviews. The focus is on understanding the experiences, benefits, and challenges the participants encounter when utilizing a risk library as part of their risk management practices.

The subsections delve into the participants' experiences, highlighting the key themes, challenges, and benefits that emerged from their accounts. Through these insights, readers can gain a deeper understanding of the practical implications and potential value of incorporating a risk library into their risk management practices. These insights offer valuable information on a risk library's role, functionality, and impact in enhancing risk management processes and outcomes, and can inform organizations considering the adoption of a risk library.

4.5.1 A Risk Library Reduces Ambiguity

Using a risk library significantly reduces ambiguity and fosters a clearer understanding of risks, as highlighted by the participants' insights. The quotes in Table 4.20 emphasize the advantages of having a risk library regarding risk understanding.

Table 4.20: Quotes Related to Reducing Ambiguity

Reference	ID	Quote
Participant A	T-1	"With a risk library, we have standardized descriptions of the risks. This ensures that people eventually develop a shared understanding of the same type of risk, as a standardized definition is available. This is a great benefit with the risk library."
Participant A	T-2	"A risk library helps the organization identify and assess risks by allowing individuals to access an overview of various types of risks. This increases awareness and helps individuals become better acquainted with what risk actually entails. The concept of risk can be somewhat abstract for those who lack experience. A risk library can help reduce this ambiguity and provide a better understanding of different types of risks."
Participant B	T-3	"I believe that a risk library helps to manage differences in risk perception. It necessitates accepting that the risks are predefined. Instead of spending a lot of time describing the risks, we can focus on discussing what they mean for us and how to manage them. This shift allows us to address the differences in risk perception more effectively."

These quotes highlight the value of a risk library in standardizing risk descriptions, promoting shared understanding, and facilitating improved risk identification and assessment processes. By providing standardized definitions and a comprehensive overview of various risk types, the risk library enables individuals to comprehend risk concepts and their implications better. Moreover, the risk library helps address differences in risk perception by establishing predefined risks, enabling more focused discussions on risk management strategies and actions.

Participant A emphasized the value of a risk library in providing standardized descriptions and definitions for different types of risks. They highlighted how having a common language and understanding of risks can contribute to better communication and alignment within the organization. A risk library promotes awareness and understanding of risks among individuals within the organization. Participant A stressed that having a centralized repository of risks enables individuals to browse through and reflect on different risk types, thereby reducing ambiguity and enhancing their comprehension of risk concepts.

Participant B underscored the significance of a risk library in managing variations in risk perception. They suggested that by having predefined risks in the library, the focus can shift from describing the risks to discussing their implications and management strategies. This approach enables more effective communication and alignment among individuals with different risk perspectives. By leveraging a risk library, organizations can promote consistency, enhance risk awareness, and foster more effective risk management practices. The centralized repository of predefined risks facilitates knowledge sharing, encourages informed decision-making, and improves risk management outcomes.

4.5.2 A Risk Library Makes the Risk Identification Phase More Efficient

The implementation of a risk library has demonstrated its ability to improve the efficiency of risk identification processes, as indicated by the insights shared by Participant B. The quotes in Table 4.21 shed light on the positive impact of a risk library on risk identification.

Using a risk library provides organizations with a repository of predefined risks, facilitating the identification process and reducing the time spent on it. By leveraging the risk library, practitioners can access standardized descriptions of risks, enabling quicker and more streamlined identification of relevant risks. This eliminates the need for repetitive and time-consuming identification efforts, allocating more time and resources to scoring, prioritizing, and managing risks and associated actions.

Table 4.21: Quotes Related to Risk Identification Efficiency

Reference	ID	Quote
Participant B	U-1	"We have created a risk library focusing on stable and secure operations. It has helped us spend less time on the identification phase and more time on scoring and prioritizing risks and actions. So, we have shifted our focus to risk management rather than identification, which everyone has positively received. We have found that while our risk library needs expansion and improvement, it still hits the mark 9 out of 10 times."
Participant B	U-2	"We follow the ISO 31000 steps in our risk management process. We spent an enormous amount of time in the risk identification phase. I almost feel embarrassed about how much time we dedicated to identifying risks. Now, with the standardized process, we spend less than half the time on the same process."

The organization has reduced the time spent identifying risks by having a comprehensive risk library that specifically addresses stable and secure operations. This time-saving benefit has allowed them to allocate more resources to scoring and prioritizing risks and developing corresponding risk management actions. By shifting its focus from identification to proactive risk management, the organization experienced positive feedback. The second quote emphasizes the transformation brought by implementing a risk library aligned with the ISO 31000 risk management framework. Before having a risk library, the organization invested significant time in the risk identification phase. However, by introducing a standardized process facilitated by the risk library, the organization observed a significant reduction in the time required for risk identification. Adopting a risk library enabled them to streamline and expedite the risk identification process, enabling the organization to operate more efficiently.

4.5.3 A Risk Library Fosters a Structured Approach to Risk Management

A risk library plays a crucial role in fostering a structured approach to risk management, as highlighted by the quotes Table 4.22.

Table 4.22: Quotes Related to Structured Risk Management Using a Risk Library

Reference	ID	Quote
Participant A	V-1	"I believe using a risk library provides a detailed overview that can contribute to several benefits. I think categorizing different types of risks makes things easier for those managing it and those who need to keep track of their deliveries. A risk library allows for better organization and a more structured approach to risk management, ultimately leading to more effective risk identification, assessment, and mitigation strategies."
Participant B	V-2	"With a risk library, you have typical risks more readily available. We can also create risk control packages that specify the relevant risks to analyze for a particular system, platform, or risk assessment. We can tailor risk assessments much more effectively."
Participant B	V-3	"We have undergone a phase where risk analyses were conducted, but the results were stored away and forgotten. We have tried simplifying the process by creating standardized risks and 'standard packages' for risk management. This enables quicker identification of risks and greater opportunities for data reuse across the organization. We have noticed that many risks and controls are repetitive. Having standard components in a risk library is incredibly valuable."

Participant A shed light on using a risk library allows for better organization and categorization of different types of risks, facilitating more effective risk identification, assessment, and mitigation. By providing a detailed overview of risks, the risk library enables practitioners to streamline the risk management process and make informed decisions based on standardized risk components.

As highlighted by Participant B, a risk library allows for the creation of risk control packages, specifying the relevant risks to be analyzed in various contexts, such as specific systems, platforms, or risk assessments. This tailored approach enhances the accuracy and efficiency of risk assessments, ensuring that the right risks are addressed in a targeted manner. Implementing a risk library also promotes consistency and data reuse across the organization. By standardizing risks and creating standardized components, organizations can quickly identify risks and leverage existing data to inform risk management practices. This approach saves time and effort by eliminating the need for repetitive risk identification and assessment processes.

4.5.4 A Risk Library Can Be Utilized to Estimate Annual Loss Expectancy (ALE)

A risk library can serve as a valuable resource for estimating the Annual Loss Expectancy (ALE), as highlighted by Participant A in the quote in Table 4.23. By leveraging the risk library, organizations can calculate the expected cost associated with specific risks and assess the potential impact on resources. This enables the organization to make informed decisions by understanding the financial implications of the risks they face. This approach gives organizations insights into the financial consequences of risks and enables them to prioritize mitigation efforts based on their potential impact.

Compared to traditional methods such as Excel, using a risk library represents a significant advancement in estimating ALE. The library provides a centralized repository of risks, ensuring accurate and up-to-date data is used in the calculation process. This enhances the accuracy and reliability of ALE estimates, enabling organizations to make more informed financial decisions regarding risk management.

Table 4.23: Quote Related to Estimation of ALE

Reference	ID	Quote
Participant A	W-1	"We use the library to estimate the ALE for a risk. We are trying to include this measure for all the risks we register as best we can. This allows us to calculate the expected ALE for each Risk Statement. For example, we can calculate the cost associated with resource-related risks. If no action is taken, we can see the estimated cost for the upcoming year. This is a big leap forward from what we could do in Excel."

4.5.5 Implementing a Risk Library Could Be Perceived as Rigid and Overly Standardized

Participant B highlighted that implementing a risk library could be met with resistance from individuals who perceive it as rigid and overly standardized, as seen in the quote in Table 4.24, and offered insight on how organizations can deal with this challenge.

Table 4.24: Quote Related to Risk Library Resistance

Reference	ID	Quote
Participant B	X-1	"We have faced some resistance because some individuals find it rigid and have raised concerns about it being too standardized, but there is always the option to create custom risks. If there are risks that don't fit well, they can also be removed. So, there is room for customization by adding new risks or removing existing ones. We have also incorporated data fields where individuals can provide their descriptions. We are also exploring the possibility of having multiple libraries or expanding the existing library to cover other areas."

Participant B highlighted that some individuals may express concerns about the library's lack of flexibility and customization options. However, it is important to note that customization is possible within the risk library framework. Organizations have the flexibility to create custom risks that align with their specific needs and remove existing risks that are not relevant. This allows for a tailored approach to risk identification and management. Furthermore, including data fields within the risk library allows individuals to provide additional descriptions or contextual information for specific risks. This allows for a more nuanced understanding of the risks and ensures that relevant details are captured.

To address the concerns and accommodate diverse requirements, Participant B highlighted exploring options to expand the risk library. This may involve the creation of multiple libraries to cover different areas or expanding the current library to include additional risk categories. These initiatives aim to enhance the risk library's usability and relevance, catering to different stakeholders' unique needs and preferences.

Chapter 5
Discussion

The preceding chapter presented the empirical findings of this thesis, which explored the challenges faced in traditional risk management practices and examined the implementation and use of ServiceNow's GRC module, along with a risk library. In this chapter, the findings will be contextualized within the broader literature study conducted and discussed in how they contribute to shedding light on the research questions posed in this thesis. By synthesizing the empirical evidence with the existing theoretical knowledge, the aim is to better understand the findings' implications, significance, and practical effects.

The chapter serves as a platform to analyze and interpret the results, drawing connections between the research questions, the empirical data, and the relevant literature. The chapter's structure is built around the research questions, which have been presented in depth in Section 1.1.1:

1. *RQ1: What are some common limitations and challenges with traditional risk management?*
2. *RQ2: To what extent could the use of ServiceNow's GRC module help solve these challenges?*
3. *RQ3: How can a standardized risk library contribute to enhancing this process?*

5.1 RQ1: What are some common limitations and challenges with traditional risk management?

The first research question aimed to identify and understand traditional risk management practices' typical limitations and challenges. Based on the interviews, the following three main categories of challenges with traditional risk management have been identified:

1. **Fragmented and Disconnected Processes**: Fragmented and disconnected processes in traditional risk management was highlighted as a considerable challenge, hindering organizations from obtaining a comprehensive and integrated view of the risk landscape, further leading to inefficiencies and inconsistencies.

2. **Manual and Time-Consuming Practices**: One of the most heavily mentioned limitations was the heavy reliance on manual processes, including data entry and manipulation, as well as the use of standalone tools such as Excel spreadsheets and Word documents. These tools lack the ability to integrate with other systems, which leads to difficulties in maintaining up-to-date information, and can cause inconsistencies or errors in data.

3. **Employee Engagement and Understanding**: The importance of ingrained risk culture and a common understanding of risk appetite was stressed in the interviews. Traditional risk management may not provide efficient stakeholder engagement mechanisms or communication of risk information across an organization. This can lead to a lack of understanding or awareness of risk management processes and outcomes.

5.1.1 Fragmented and Disconnected Processes

As revealed by the interviews, traditional risk management practices often exhibit a fragmented and inefficient nature. They often operate in silos, focusing on specific risks or categories of risks. This approach can lead to a narrow understanding of the risk landscape, preventing a comprehensive and integrated view of the overall risks that an organization may face. The use of multiple tools, such as Word, Excel, and specialized risk analysis software, was highlighted, leading to a disjointed and non-integrated risk management process. Participant B emphasized the challenges of switching between different tools, resulting in a fragmented and independent approach to risk management. Quote D-1 in Section 4.2.4 exemplifies this aspect. This quote highlights the challenges of fragmented practices in traditional risk management approaches. Using multiple tools for different aspects of risk management leads to a lack of integration and interconnectivity.

Participant B expressed the difficulties of operating in information silos, limited collaboration, and the inability to aggregate and synthesize risk-related data and insights effectively. Various departments often have their own methods and tools for managing risk. This siloed approach can result in duplication of efforts, inconsistent risk assessments, and a lack of centralized visibility into the overall risk landscape. When each department operates independently, it becomes challenging to establish a holistic view of risks across the organization. Risk-related information is scattered, and without adequate enterprise risk reporting, leadership can struggle to include risk considerations when developing company-wide strategy [Ser23c]. Siloed risk management practices hamper collaboration, sharing knowledge, and identifying systemic risks [KM12]. Consequently, decision-making may be hindered, and the ability to prioritize and allocate resources effectively becomes compromised. This underscores the need to establish and implement a unified risk management methodology and process. Doing so would promote consistency in how risks are identified, assessed, mitigated, and reported across all levels of the organization, leading to a more integrated and effective approach to risk management.

The findings from the interviews support the existing literature, which emphasizes the importance of integration and coordination in effective risk management. GRC activities have traditionally been spread around the organization, with no overall organization or coordination [Man17; AF20]. Fragmented risk management processes can result in suboptimal coordination, inefficient resource allocation, and difficulty aggregating risk information [TBDM14]. Furthermore, the lack of integration between risk management tools and processes inhibits organizations from achieving a holistic and coherent understanding of risk [HT21]. Without a structured approach and broader understanding of risks, organizations could miss critical interconnections and potential cascading effects of various risks [BCH05b].

On the other hand, some traditional risk management tools may offer specific functionalities that cater to certain aspects of risk analysis. For instance, specialized risk analysis software mentioned by Participant B (Quote D-1, Section 4.2.4) could provide in-depth analysis capabilities for particular risk areas. However, these tools are often limited to certain users or departments, further contributing to fragmentation and disconnected processes. A disconnected ecosystem where multiple risk management systems are not unified may cause issues [RS23]. It can make it difficult to ascertain information about the organization, whether determining new or changing risks or where similar processes and activities are taking place across the organization to mitigate similar risks.

Additionally, the interviews highlighted that risk data management is often concentrated in the hands of a few individuals. Participant A mentioned they would manage the entire Excel spreadsheet on behalf of everyone. This centralized

approach limits the participation and engagement of other individuals within the organization, potentially leading to delays, lack of ownership, and inefficiencies in identifying, assessing, and mitigating risks [HT21]. It also hinders transparency, as other stakeholders may not have direct access to the risk information, limiting their ability to understand and respond to risk effectively. Quotes C-1 and C-2 in Section 4.2.3 highlight this. The concentration of risk data management in the hands of a few individuals can hinder the organization's risk management efforts [HT21]. Reliance on a single person to manage the entire risk data spreadsheet places considerable pressure on that individual. It may introduce potential errors or delays in updating and maintaining the risk information [TBDM14].

Traditional risk management processes' fragmented and disconnected nature poses challenges to effective risk assessment, analysis, and decision-making. The existing literature and empirical data provide evidence of the limitations and inefficiencies associated with fragmented risk management. Integrated risk management solutions offer the potential to address these challenges by providing a centralized platform for risk-related activities. However, implementing such solutions requires careful planning, resource allocation, and effective change management strategies.

5.1.2 Manual and Time-Consuming Processes

A recurring theme in both interviews was the limitations and challenges associated with manual processes and reporting in traditional risk management systems. Traditionally, risks are managed with largely qualitative and manual assessments. Their periodic and static applications limit the effectiveness of these tools, the subjective biases of individual assessors, and their reactive and backward-looking nature [CBG+23]. Both interviewees highlighted the time-consuming nature of these tasks and their subsequent impact on the ability to manage risks effectively. Such manual handling of data and reports makes the process less efficient, leading to difficulty maintaining consistency and accuracy, and restricts the capacity for effective reusability of the work, as highlighted in quotes A-1 and A-5 in Section 4.2.1. Both participants expressed concern regarding the limitations when coping with large data volumes.

Quote B-1 in Section 4.2.2 emphasizes the difficulty of synthesizing and analyzing risk data from various parts of the organization to create a holistic view of the risk landscape. When relying on manual processes and fragmented systems, obtaining a comprehensive view of risks across the entire organization becomes challenging. Employees are often forced to create overviews and reports, which are mostly compiled in a manual procedure, by themselves [TBDM14]. This, again, is error-prone as it easily causes inconsistencies. Manually aggregating data from various sources and attempting to analyze risks in isolation can hinder identifying patterns, trends, and

interdependencies. This limitation hampers the organization's capacity to make informed decisions and proactively mitigate risks.

Relying on spreadsheets or manual systems to manage risks hampers the ability to handle large amounts of data efficiently. Scrolling through a spreadsheet to gain a comprehensive overview of risks is time-consuming, cumbersome, and prone to errors [AF20; TBDM14], as also highlighted in quotes A-1 and A-4 in Section 4.2.1 and quotes B-1 and B-3 in Section 4.2.2. Moreover, the lack of reusability in manual methods makes it challenging to scale the risk management process as the number and complexity of risks increase [Serd]. This repetitiveness also wastes time and effort, as much of the work cannot be effectively utilized in subsequent analyses or reporting.

The limitations of traditional risk management tools in handling real-time data and their dependence on manual data analysis and reporting can significantly decrease efficiency. These manual processes can be time-consuming, inefficient, and susceptible to human error, which might lead to inconsistencies and inaccuracies in risk reporting. These tools also lack the ability to integrate with other systems, which leads to difficulties in maintaining up-to-date information, and can cause inconsistencies or errors in data. Adopting more scalable and automated risk management tools and practices can streamline processes, improve data handling capabilities, and enable organizations to manage risks effectively [ATRC19; GNW12]. Incorporating digital solutions, such as risk management software, can enhance efficiency, reduce manual efforts, and provide better insights for decision-making [AF20].

The findings highlight the limitations and challenges of manual and time-consuming processes in traditional risk management. These challenges necessitate adopting more efficient and automated risk management tools and practices to streamline processes, enhance productivity, and improve the overall effectiveness of risk management activities. Frequently, manual processes need more flexibility and agility to manage growing data volumes and complexity. Automated systems allow for real-time data collection, analysis, and reporting, thereby providing stakeholders with timely insights for sensible decision-making. Automation reduces the burden of manual processes, facilitating more efficient resource allocation and a comprehensive and streamlined approach to risk management. Moreover, digital platforms provide dynamic dashboards and visualizations that improve enterprise-wide risk communication and comprehension.

5.1.3 Employee Engagement and Understanding

Establishing a robust risk culture is crucial for effective organizational risk management. Both interviewees emphasized the significance of risk culture and highlighted the challenges associated with fostering a strong risk culture (Quotes E-1, E-2, and E-3 in Section 4.2.5. This involves getting people to understand the value of risk management and integrating it into decision-making processes.

Building a strong risk culture requires creating an environment where risk management is embedded in everyday operations, decision-making processes, and employee mindsets. Effective communication, training programs, and continuous reinforcement are vital in promoting risk awareness, accountability, and a proactive approach to risk management. By addressing the challenges associated with risk culture, organizations can empower employees to actively participate in risk management processes and contribute to the overall effectiveness of the risk management framework.

Another significant challenge highlighted by the interviewees is the difficulty in defining and communicating the organization's risk appetite and acceptance criteria. It is critical to establish a clear understanding of these parameters as they set the framework for risk management decisions. Traditional methods, often limited to a few individuals, contribute to a lack of understanding and engagement in the risk management process, hindering the establishment of a robust risk culture within the organization. To develop an effective risk management system, a clear formulation and communication of the firm's risk appetite is required [KM16]. It is essential to understand risk appetite in a dynamic organizational process [Pow09]. Without a well-defined and understood risk appetite, it becomes challenging for an organization to make informed risk-related decisions [Bea17]. Hence, as quote E-2 in Section 4.2.5 points out, the lack of a clear understanding of what risk entails and the organization's risk appetite can be seen as a significant limitation of traditional risk management approaches.

The inherent complexity in defining risk appetite and acceptance criteria can lead to inconsistencies in risk assessment across different parts of the organization, with different parts potentially adopting varying standards. This inconsistency can result in suboptimal risk management decisions and misalignment with the organization's risk tolerance. Educating and raising awareness among employees about risk-related matters is essential in cultivating a shared understanding of risk and risk appetite within the organization, and building risk awareness among employees requires ongoing efforts and creating an environment where risk conversations are part of the norm [Pow09].

Fostering a risk-aware culture requires ongoing efforts beyond providing training programs. It involves creating an environment where risk conversations are normalized

and employees understand their role in managing risk. Building risk awareness among employees is not just about knowledge transfer but involves creating a culture where risk considerations are integrated into daily operations and decision-making processes. When employees lack understanding about what risk entails, it hampers their ability to manage and mitigate risks effectively. Organizations can promote risk awareness and engagement by educating employees about the nature of risk, its potential impact on the organization, and the importance of risk management practices.

Addressing the challenges associated with employee engagement and understanding risk management is essential for developing a strong risk culture. By fostering a risk-aware culture and ensuring that employees clearly understand risk concepts and their role in managing risks, organizations can enhance their risk management effectiveness and create a more resilient and proactive approach to addressing risks.

5.2 RQ2: To what extent could the use of ServiceNow's GRC module help solve these challenges?

By examining the interviewees' experiences and perspectives, this research question aimed to understand the impact of ServiceNow's GRC module in addressing the identified challenges and enhancing risk management. Their narratives explore how ServiceNow's GRC module has influenced the efficiency of processes, the breadth and depth of risk management practices, and the engagement and understanding of employees.

The subsequent sections will delve into the potential of ServiceNow's GRC module in addressing the challenges identified in RQ1, based on insights gained from the interviews.

5.2.1 Addressing Fragmented and Disconnected Processes

ServiceNow's GRC module offers a comprehensive solution to address the challenges of fragmented and disconnected risk management processes. The module enables organizations to integrate and streamline their risk management activities by providing a centralized platform, eliminating the need for multiple tools and disjointed approaches.

The centralized nature of the GRC module eliminates the need for switching between different tools, such as Word, Excel, or specialized risk analysis software. Organizations can streamline their risk management processes by leveraging the module's functionalities, which include risk registers, automated data aggregation, and real-time reporting. This reduces manual efforts, minimizes the potential for errors and inconsistencies, and enhances efficiency in managing risks. It also allows

for broader participation and engagement of individuals within the organization by granting them access to risk information and enabling them to contribute to risk management efforts. This distributed approach enhances transparency, ownership, and accountability, reducing reliance on a single person for risk data management. Organizations can leverage their expertise and perspectives by involving a wider range of stakeholders, leading to more comprehensive risk assessments and more effective risk mitigation strategies.

With ServiceNow's GRC module, organizations can establish a unified risk management methodology and process that spans across departments and functions. The module allows for consistent risk identification, assessment, mitigation, and reporting practices, ensuring a holistic and coherent understanding of risks across the organization. By standardizing and centralizing risk management processes, organizations can avoid duplication of efforts, improve coordination, and enhance resource allocation efficiency. It provides tools and functionalities for communicating risk appetite, setting risk tolerances, and aligning risk management activities with strategic objectives. Organizations can coordinate risk management practices to their specific requirements by customizing the module's workflows and approval processes. This promotes a more integrated and effective approach to risk management.

Moreover, the module promotes collaboration and knowledge sharing by providing a shared platform for risk-related activities. The GRC module consolidates risk-related data, assessments, and controls into a single system. This centralization enables better coordination and collaboration among different departments and stakeholders involved in risk management [Bhi09]. Rather than working in isolation, the module promotes a more integrated approach to risk management, where all stakeholders have access to up-to-date risk information. This facilitates better communication, knowledge sharing, and identifying systemic risks. It also promotes transparency, ownership, and accountability among stakeholders, who can directly contribute to risk assessments, update risk information, and participate in decision-making. The module provides role-based access controls, ensuring individuals have appropriate access levels and responsibilities within the risk management process.

In the absence of an integrated system, obtaining comprehensive views and specific data required manual efforts and extensive scrolling through spreadsheets or documents. The GRC module provides real-time visibility into the overall risk landscape through dashboards and reports. This enables stakeholders at all levels to monitor risk status, track mitigation activities, and make informed decisions based on up-to-date information. By having a centralized and accessible view of risks, organizations can identify emerging risks, evaluate their impact, and take proactive measures to address them. Improved visibility and understanding of risks across the organization contribute to a more comprehensive enterprise-wide view.

However, it is important to acknowledge that effective process integration relies on good data quality and structure. Establishing a solid foundation with accurate and reliable information about risks and resources is crucial to leverage the process integration capabilities of the GRC module. Organizations need to ensure that data is consistently updated, validated, and properly structured to maximize the benefits of process integration in risk management.

ServiceNow's GRC module helps solve the challenges of fragmented and disconnected processes in traditional risk management by providing a centralized platform. The module enables better coordination, collaboration, and decision-making by consolidating risk data and promoting a more integrated approach to risk management. It streamlines processes, eliminates the need for multiple tools, and facilitates broader participation and engagement in risk management efforts, granted the data quality is up to a certain standard. By leveraging the benefits of the GRC module, organizations can overcome the limitations of fragmented risk management and achieve more efficient and effective risk management practices.

5.2.2 More Efficient and Less Time-Consuming Processes

In the interviews conducted, one of the key challenges identified in traditional risk management was the heavy reliance on manual processes, such as data entry and manipulation. These manual processes consumed valuable time and introduced potential errors and inconsistencies. Adopting more scalable and automated risk management tools and practices can streamline processes, improve data handling capabilities, and enable organizations to manage risks effectively [ATRC19]. Incorporating digital solutions, such as risk management software, can enhance efficiency, reduce manual efforts, and provide better insights for decision-making [GNW12]. Centralized risk registers, automated data aggregation, real-time reporting, and customizable dashboards allow for easier risk assessment and monitoring.

ServiceNow's GRC module addresses the challenges associated with manual and time-consuming processes by offering automation and streamlining capabilities, reducing reliance on manual tasks, and improving efficiency. The organization can then focus on work that requires interpretation and insight, not repetitive tasks [Del20], enabling broader, deeper, more forward-looking views of risks. Organizations can save time and effort by automating data collection, analysis, and reporting. Real-time data handling is another key feature of the GRC module, enabling organizations to have up-to-date risk information readily available. This eliminates the need for manual data entry and manipulation, reducing the risk of errors and inconsistencies.

The GRC module facilitates integration and data consolidation. It allows for integrating risk data from various sources and systems, consolidating them into a centralized platform. This eliminates the need for manual data aggregation

from multiple tools and spreadsheets, saving time and reducing the risk of data inconsistencies. Integrating and consolidating data provides a comprehensive view of the organization's risk landscape, enabling better risk analysis and decision-making. Dynamic dashboards and visualizations further improve risk communication and comprehension. Organizations can generate reports easily and quickly, presenting risk information clearly and visually appealingly. These visual representations make it easier for stakeholders to understand complex risk data, facilitating more effective risk discussions and decision-making processes.

Additionally, the GRC module brings a significant shift in the organization's ability to track historical data and gain valuable insights. Unlike the previous use of Excel, where closed risk cases lacked specific linkages, the GRC module enables the establishment of meaningful connections and associations. The module enables users to link cases to specific Risk Statements, log assessments, and track and close actions in a structured manner. The enhanced historical tracking within the GRC module allows organizations to analyze risk data over time and derive valuable insights. It eliminates the need for extensive manual work and facilitates a more streamlined and automated approach to tracking risk-related information.

Scalability and reusability are other benefits of ServiceNow's GRC module. As risks become more numerous and complex, the module allows organizations to scale their risk management processes efficiently. The automated and centralized nature of the module enables handling large amounts of data without sacrificing efficiency. Additionally, the module promotes the reusability of risk management work, ensuring that efforts put into risk assessment and analysis can be effectively utilized in subsequent analyses or reporting. This eliminates repetitive tasks and optimizes the use of resources.

ServiceNow's GRC module addresses the challenges of manual and time-consuming processes in risk management by offering automation, real-time data handling, integration, enhanced reporting, and scalability. Flexibility in the module ensures that it can grow and adapt to the organization's evolving risk management needs. By leveraging these features, organizations can streamline risk management processes, improve efficiency, and make more informed decisions.

5.2.3 Building a Robust Risk Culture

By providing a centralized platform for risk management activities, the GRC module encourages employees to actively participate in the risk management process. It facilitates communication and collaboration, allowing stakeholders to contribute their insights and expertise. This promotes a culture where risk management is seen as a collective responsibility, and employees understand the value of accepting and actively managing risks. Through effective communication channels and training programs, the module helps raise risk awareness and promotes a proactive approach to risk management. This promotes open communication and knowledge exchange, fostering a culture of risk awareness and engagement throughout the organization.

The integration of risk information is a crucial feature of the GRC module. It supports the definition and communication of risk appetite and acceptance criteria by providing a framework for defining these parameters and ensuring that they are integrated into the risk management process. Organizations can establish clear risk appetite statements using the module's functionalities and communicate them effectively to employees. This clarity helps align employees' actions with the organization's risk tolerance and promotes consistent risk management practices. Employees can make informed decisions regarding risk management by understanding the organization's risk appetite and the criteria for accepting or mitigating risks. By having access to integrated risk information, employees can better understand the interconnectedness of risks and identify potential dependencies.

Furthermore, the module facilitates transparency and accessibility of risk-related information. Instead of having risk data concentrated in the hands of a few individuals, the module allows for broader access to risk information. This enhances transparency and empowers employees to understand and respond to risks effectively. By providing a centralized platform for risk data, assessments, and controls, the module enables employees to access up-to-date risk information and contribute their insights. This inclusivity promotes engagement and ownership of risk management processes, leading to more effective risk mitigation and decision-making.

ServiceNow's GRC module helps address the challenges related to employee engagement and understanding in traditional risk management by fostering a robust risk culture through promoting active participation and raising risk awareness among employees. The module supports defining and communicating risk appetite and acceptance criteria, ensuring alignment with the organization's risk tolerance. It also enhances transparency and accessibility of risk-related information, empowering employees to make informed decisions and actively contribute to risk management efforts.

5.2.4 Considerations for Implementing ServiceNow's GRC Module

While ServiceNow's GRC module offers numerous benefits, organizations should consider several factors when implementing the module to ensure successful adoption and utilization.

Before implementing the GRC module, organizations should assess their readiness in terms of risk management maturity, organizational culture, and change management capabilities. Adequate preparation, including defining clear goals, engaging stakeholders, and addressing any cultural or organizational barriers, is crucial for a smooth implementation process. Implementing a GRC module involves introducing changes to existing processes, systems, and workflows. Organizations must assess their change management capabilities to ensure a smooth transition and adoption of the GRC module. Organizations with a higher risk management maturity level are likely to have well-defined risk governance structures, established risk appetite and tolerance levels, and standardized risk assessment and mitigation practices. They may be better positioned to leverage the capabilities of a GRC module and achieve more significant benefits from its implementation.

Organizations should invest in adequate preparation before introducing the GRC module to ensure a smooth implementation process. This preparation includes defining clear goals and objectives for the GRC module implementation, engaging key stakeholders, and addressing any cultural or organizational barriers hindering adoption. Defining clear goals helps align the implementation efforts with the organization's strategic objectives and ensures that the GRC module implementation is focused and purposeful. Engaging relevant stakeholders fosters ownership, increasing the chances of successful implementation and adoption. Thorough planning and involvement of the stakeholders are essential to ensure that the module accurately reflects the organization's risk management practices. Organizations should regularly evaluate and improve their risk management practices, leveraging the insights and capabilities provided by the GRC module.

Further, providing users with comprehensive training and ongoing support is essential for effectively utilizing the GRC module. Employees should receive training on the module's features, functionalities, and best practices for risk management. Ongoing support and communication channels should be established to address user questions, provide guidance, and facilitate continuous improvement.

Integration and Organizational Alignment

The superiority of ServiceNow is not solely attributed to the tool itself but rather to the level of integration and organizational alignment it offers. This underscores the

significance of integration and alignment within the organization when implementing any GRC tool, including ServiceNow's GRC module. The tool's effectiveness lies not only in its features and functionalities but also in its seamless integration into existing processes and workflows. When risk management is embedded throughout the organization and incorporated into daily operations, the choice of the GRC tool becomes less about the tool itself and more about its compatibility with the organization's overall structure and systems.

Organizational alignment ensures that risk management practices are consistently applied, and all stakeholders are engaged. It enables a holistic view of risks and facilitates communication, collaboration, and accountability across departments. Therefore, while ServiceNow's GRC module may offer specific advantages and capabilities, its true value is maximized when it is part of a broader organizational commitment to risk management.

5.3 RQ3: How can a standardized risk library contribute to enhancing this process?

Standardization plays a crucial role in effective risk management practices. A risk library provides a structured and consistent framework for identifying, categorizing, and assessing risks. It serves as a repository of predefined risk types, descriptions, and associated controls, ensuring a common understanding and language for risk management across the organization.

A risk library offers several benefits in enhancing the risk management process. Firstly, it promotes efficiency and consistency in risk identification and assessment. Organizations can streamline the risk identification phase by having a predefined set of risk categories and descriptions, ensuring that all relevant risks are considered. This eliminates the ad-hoc nature of risk identification and reduces the likelihood of overlooking important risks. It also reduces subjectivity and bias in risk assessment, leading to more reliable and comparable risk ratings. Standardized risk assessment criteria also facilitate risk prioritization, helping organizations allocate resources and focus on the most significant risks.

Another advantage of a standardized risk library is the ability to leverage industry best practices. It allows organizations to incorporate established risk frameworks, guidelines and benchmarks into their risk management processes. Organizations can benefit from collective wisdom and industry experience by aligning with recognized standards and practices. This promotes adopting leading practices, improves risk management effectiveness, and enhances the organization's risk management maturity.

ServiceNow's GRC module offers a standardized risk library as part of its capa-

bilities through Risk Statements. This provides a comprehensive set of predefined risk types, descriptions, and associated controls, enabling organizations to establish a standardized risk framework quickly. The organization can customize the risk library to align with its specific industry, regulatory requirements, and internal risk management practices. Having an inventory of all risks and controls in a centralized repository or risk universe makes it easier to aggregate risks at various levels of the hierarchy, providing visibility into the areas that need focus [Ser22]. Organizations can streamline their risk management processes and promote consistency and efficiency by utilizing ServiceNow and a risk library. The predefined risk types and descriptions facilitate identifying and assessing risks, ensuring that no critical risks are overlooked. Objective and consistent risk evaluations are easier carried out, enhancing the organization's ability to prioritize risks and allocate resources effectively.

However, introducing a standardized risk library and a new risk management process may require a change in management efforts to promote user adoption and engagement. Some employees may resist the transition or struggle to adapt, affecting the overall effectiveness of the risk management process. Keeping the risk library up-to-date and relevant can also be an ongoing challenge. Changes in industry regulations, emerging risks, or organizational priorities may require regular updates to the risk library and associated controls. Adequate resources and processes need to be in place to ensure timely maintenance.

A risk library enhances the risk management process by providing a structured and consistent framework for risk identification, assessment, and prioritization. It promotes efficiency, consistency, and the adoption of industry best practices. ServiceNow's GRC module offers a standardized risk library as part of its capabilities, enabling organizations to establish a standardized risk framework and improve their risk management practices. This improves the quality and effectiveness of risk management activities and enhances the organization's ability to respond to risks.

5.4 Threats to Validity

The thesis is based on information gathered from semi-structured interviews. As there were only two interviewees, when asking a follow-up question or something outside of the interview guide, only one answer on this topic was available for analysis. Having only one or two answers to base the analysis and discussion on also implies that it is likely that the discussion is somewhat biased by the interviewees' perspectives. Despite this, it has been made a conscious effort to remain objective.

Chapter 6
Conclusion and Future Work

The thesis has explored the significance and role of ServiceNow's GRC module and a standardized risk library in solving organizational risk management challenges. The conducted interviews and the analysis of various academic and industry sources provide compelling insights into how ServiceNow's GRC module can serve as a comprehensive solution to enhance risk management efficiency and effectiveness.

ServiceNow's GRC module offers several benefits, including streamlined workflows, centralization, automation, and integration of risk management processes. It enables organizations to reduce operational silos and foster a holistic, company-wide approach to risk management. The GRC module promotes a proactive stance towards risk management, with predictive analytics capabilities and real-time dashboards. This empowers organizations to promptly identify and address potential risks and non-compliance issues, mitigating adverse impacts and fostering a resilient organizational structure.

A standardized risk library further enhances the risk management process by promoting consistency and efficiency in risk identification, assessment, and prioritization. It ensures that a common understanding and language of risk management exists across the organization, reducing subjectivity and bias in risk assessments and facilitating effective resource allocation. Incorporating recognized standards and practices also allows organizations to leverage industry best practices and enhance their risk management maturity.

However, successfully implementing and utilizing ServiceNow's GRC module and a risk library requires careful consideration and preparation. Factors such as the organization's risk management maturity, organizational culture, and change management capabilities significantly influence the success of these tools. Clear goals and objectives for implementation, stakeholder engagement, and adequate user training are crucial for ensuring a smooth transition and promoting user adoption.

The results of this thesis emphasize the potential of ServiceNow's GRC module and a standardized risk library as tools for enhancing risk management within organizations. Nevertheless, it's crucial to keep in mind that these tools are only as effective as the organizational commitment towards risk management. They offer powerful capabilities, but their success relies heavily on an organization-wide commitment to risk management, a culture that encourages transparency and accountability, and a readiness to adapt and evolve.

6.1 Future Work

The research presented in this thesis provides valuable insights into the application and benefits of ServiceNow's GRC module and a standardized risk library in risk management processes. However, there are several potential areas for future research:

Comparative Study

A comparative study involving ServiceNow's GRC module and other GRC tools could offer valuable insights into the strengths and weaknesses of different platforms. Such research would provide more comprehensive guidance to organizations seeking to adopt or switch to a new GRC platform.

In-depth Study of ServiceNow's GRC Module in Different Industries

Future research could investigate the application and effectiveness of ServiceNow's GRC module across different industries. This could help understand how industry-specific regulations and risk landscapes influence the implementation, customization, and utilization of ServiceNow's GRC module.

Development of Standardized Risk Libraries

The thesis highlighted the importance of standardized risk libraries in enhancing risk management processes. Future work could focus on developing comprehensive and adaptable risk libraries for various industries and risk landscapes. These could be periodically updated based on emerging risks and changes in regulatory environments.

These potential research avenues could significantly contribute to the existing body of knowledge on GRC tools, their implementation, and their impact on risk management processes in organizations.

References

[AF20] R. J. Anderson and M. L. Frigo, «Understanding and Implementing Enterprise Risk Management», *Committee of Sponsoring Organizations of the Treadway Commission*, 2020.

[ASM23] M. Adam, A. M. Soliman, and N. Mahtab, «Measuring enterprise risk management implementation: A multifaceted approach for the banking sector», *The Quarterly Review of Economics and Finance*, vol. 87, pp. 244–256, Feb. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1062976921000028.

[ATRC19] N. Albinson, C. Thomas, *et al.*, «Future of risk in the digital era | Transformative change. Disruptive risk.», *Deloitte*, 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-future-of-risk-in-the-digital-era-report.pdf.

[Ave15] T. Aven, *Risk Analysis*. John Wiley & Sons, 2015.

[AVS20] S. A. Arutyunov, E. N. Voskresenskaya, and L. S. Scherbakova, «Corporate Governance and Compliance with the View of IT Companies», in *Proceedings of the International Conference on Software Engineering and Information Management (ICSIM)*, 2020, pp. 167–173.

[AWV20] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, «Information security governance challenges and critical success factors: Systematic review», *Computers & Security*, vol. 99, p. 102 030, Dec. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820303035.

[BCH05a] M. Beasley, R. Clune, and D. R. Hermanson, «Enterprise Risk Management's Wake-up Call: Demonstrations of Risk Management's Benefit», *Balance Sheet*, vol. 13, no. 2, pp. 20–26, 2005.

[BCH05b] M. S. Beasley, R. Clune, and D. R. Hermanson, «Enterprise risk management: An empirical analysis of factors associated with the extent of implementation», *Journal of Accounting and Public Policy*, vol. 24, no. 6, pp. 521–531, Nov. 2005. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278425405000566.

[Bea17] M. S. Beasley, *Today's Risk Management Challenges: It's a Small World After All*, Jul. 2017. [Online]. Available: https://erm.ncsu.edu/library/article/todays-risk-management-challenges-its-a-small-world-after-all.

[Bhi09] A. Bhimani, «Risk management, corporate governance and management accounting: Emerging interdependencies», en, *Management Accounting Research*, Risk Management, Corporate Governance and Management Accounting, vol. 20, no. 1, pp. 2–5, Mar. 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1044500508000565.

[BMNR15] P. Bromiley, M. McShane, *et al.*, «Enterprise Risk Management: Review, Critique, and Research Directions», *Long Range Planning*, vol. 48, no. 4, pp. 265–276, 2015.

[CBG+23] N. Cornwell, C. Bilson, *et al.*, «Modernising operational risk management in financial institutions via data-driven causal factors analysis: A pre-registered report», *Pacific-Basin Finance Journal*, vol. 77, Feb. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0927538X22002013.

[Cre13] J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage publications, 2013.

[CW11] C. Chapman and S. Ward, *How to Manage Project Opportunity and Risk: Why Uncertainty Management Can Be a Much Better Approach than Risk Management*. John Wiley & Sons, 2011.

[Del20] Deloitte, «World Class Risk Assurance | Connect. Modernise. Digitise», 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/audit/IA-Connect-Modernize-and-Digitize.pdf.

[For18] Forbes, *The World's Most Innovative Companies*, 2018. [Online]. Available: https://www.forbes.com/innovative-companies/list/ (last visited: Jul. 8, 2023).

[GNW12] S. Gates, J.-L. Nicolas, and P. Walker, «Enterprise Risk Management: A Process for Enhanced Management and Improved Performance», *Management Accounting Quarterly*, vol. 13, Jan. 2012.

[HDLL20] J. Huang, A. Ding, *et al.*, «Increasing the risk management effectiveness from higher accuracy: A novel non-parametric method», *Pacific-Basin Finance Journal*, vol. 62, p. 101 373, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0927538X20300263.

[HM17] D. Hillson and R. Murray-Webster, *Understanding and Managing Risk Attitude*. Routledge, 2017.

[HS16] D. W. Hubbard and R. Seiersen, *How to Measure Anything in Cybersecurity Risk*. John Wiley & Sons, 2016.

[HT21] P. Hopkin and C. Thompson, *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*, 6th ed. Kogan Page Publishers, 2021.

[Hub10] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons, 2010.

[Hun21] A. Hunt, *The Critical Role Risk Libraries Play in Risk Management Successes*, Apr. 2021. [Online]. Available: https://www.360factors.com/blog/the-critical-role-risk-libraries-play-in-risk-management-successes/ (last visited: Jul. 6, 2023).

[Int18] International Organization for Standardization, *NS-ISO 31000:2018 – Risk Management – Guidelines (Norwegian version)*, Standard Norge, 2018.

[Int22] International Organization for Standardization, *NS-ISO/IEC 27005:2022 – Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks*, Standard Norge, 2022.

[KM12] R. S. Kaplan and A. Mikes, «Managing Risks: A New Framework», *Harvard Business Review*, Jun. 2012. [Online]. Available: https://hbr.org/2012/06/managing-risks-a-new-framework (last visited: Jul. 6, 2023).

[KM16] R. S. Kaplan and A. Mikes, «Risk Management—the Revealing Hand», en, *Journal of Applied Corporate Finance*, vol. 28, no. 1, pp. 8–18, 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/jacf.12155.

[KPM23] KPMG, *Is your legacy GRC tool holding you back?*, 2023. [Online]. Available: https://www.kpmg.us/content/dam/alliances/pdfs/2023/legacy-grc-tool-holding-back.pdf (last visited: Jul. 1, 2023).

[LH03] A. P. Liebenberg and R. E. Hoyt, «The Determinants of Enterprise Risk Management: Evidence from the Appointment of Chief Risk Officers», *Risk Management and Insurance Review*, vol. 6, no. 1, pp. 37–52, 2003.

[Man17] S. Mansfield-Devine, «Data governance: Going beyond compliance», *Computer Fraud & Security*, vol. 2017, no. 6, pp. 12–15, Jun. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372317300520.

[MC17] McKinsey and Company, *The future of risk management in the digital era*, Dec. 2017. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-risk-management-in-the-digital-era (last visited: Jul. 6, 2023).

[Mik09] A. Mikes, «Risk management and calculative cultures», *Management Accounting Research*, Risk Management, Corporate Governance and Management Accounting, vol. 20, no. 1, pp. 18–40, Mar. 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1044500508000450.

[MK15] A. Mikes and R. S. Kaplan, «When One Size Doesn't Fit All: Evolving Directions in the Research and Practice of Enterprise Risk Management», *Journal of Applied Corporate Finance*, vol. 27, no. 1, pp. 37–40, 2015.

[Nor] Norwegian Agency for Shared Services in Education and Research, *Sikt – Kunnskapssektorens tjenesteleverandør*. [Online]. Available: https://sikt.no/ (last visited: Jul. 5, 2023).

[PB20] S. G. Powell and K. R. Baker, *Business Analytics: The Art of Modeling with Spreadsheets*. John Wiley & Sons, 2020.

[PN02] F. D. Patterson and K. Neailey, «A Risk Register Database System to aid the management of project risk», *International Journal of Project Management*, vol. 20, no. 5, pp. 365–374, Jul. 2002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0263786301000400.

[Pow09] M. Power, «The risk management of nothing», *Accounting, Organizations and Society*, vol. 34, no. 6, pp. 849–855, Aug. 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0361368209000580.

[Pri22] PricewaterhouseCoopers, *Cyber: GRC-teknologi kan gi bedre risikostyring*, Oct. 2022. [Online]. Available: https://www.pwc.no/no/pwc-aktuelt/cyber-grc-teknologi-kan-gi-bedre-risikostyring.html (last visited: Jul. 6, 2023).

[RCD+22] O. Rodríguez-Espíndola, S. Chowdhury, *et al.*, «Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing», *Technological Forecasting and Social Change*, vol. 178, May 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162522000944.

[RIM18] RIMS, *An Overview of Widely Used Risk Management Standards and Guidelines*, Risk Management Society (RIMS), 2018. [Online]. Available: https://www.rims.org/resources/erm-resources/overview-of-erm-standards.

[Ris23] RiskOptics, *What is a Risk Register?*, Apr. 2023. [Online]. Available: https://reciprocity.com/resources/what-is-a-risk-register/ (last visited: Jul. 6, 2023).

[RS23] S. Reiss and K. Samir, *IRM+: A new approach toward technology-enabled risk management*, May 2023. [Online]. Available: https://www.ey.com/en_us/banking-capital-markets/irm-technology-enabled-risk-management (last visited: Jul. 6, 2023).

[SAY13] P. Shamala, R. Ahmad, and M. Yusoff, «A conceptual framework of info structure for information security risk assessment (ISRA)», *Journal of Information Security and Applications*, SETOP'2012 and FPS'2012 Special Issue, vol. 18, no. 1, pp. 45–52, Jul. 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221421261300029X.

[SBJ+20] N. Sukhija, E. Bautista, *et al.*, *Event Management and Monitoring Framework for HPC Environments using ServiceNow and Prometheus*. Nov. 2020. [Online]. Available: https://escholarship.org/uc/item/7ch6t25w.

[Sera] ServiceNow, *Governance, Risk, and Compliance (GRC)*. [Online]. Available: www.servicenow.com/products/governance-risk-and-compliance.html.

[Serb] ServiceNow, *ServiceNow - Now Learning*, ServiceNow Learning Platform. [Online]. Available: https://nowlearning.servicenow.com/.

[Serc] ServiceNow, *ServiceNow – The world works with ServiceNow™*. [Online]. Available: https://www.servicenow.com/ (last visited: Jul. 6, 2023).

[Serd] ServiceNow, *What is GRC? - Governance, Risk and Compliance*. [Online]. Available: https://www.servicenow.com/products/governance-risk-and-compliance/what-is-grc.html (last visited: Jul. 6, 2023).

[Ser22] ServiceNow, *ServiceNow Risk Management*, 2022. [Online]. Available: https://www.servicenow.com/standard/resource-center/data-sheet/ds-risk-management.html (last visited: Jul. 11, 2023).

[Ser23a] ServiceNow, *GRC: Advanced Risk Assessment for Implementers – On-Demand Course*, ServiceNow Learning Platform, 2023. [Online]. Available: https://nowlearning.servicenow.com/lxp?id=learning_course_prev&course_id=4667ff5bdb89209013049a82ca9619cf.

[Ser23b] ServiceNow, *GRC: Classic Risk Assessment Fundamentals – On-Demand Course*, ServiceNow Learning Platform, 2023. [Online]. Available: https://nowlearning.servicenow.com/lxp?id=learning_course_prev&course_id=28e245c91b4a38d0b9a2cae3604bcbd2.

[Ser23c] ServiceNow, *GRC: Integrated Risk Management (IRM) Fundamentals – On-Demand Course*, ServiceNow Learning Platform, 2023. [Online]. Available: https://nowlearning.servicenow.com/lxp?id=learning_course_prev&course_id=9fe7eaaf977a91908934b67e6253af36.

[Ser23d] ServiceNow, *GRC: Integrated Risk Management (IRM) Implementation On Demand – On-Demand Course*, ServiceNow Learning Platform, 2023. [Online]. Available: https://nowlearning.servicenow.com/lxp?id=learning_course_prev&course_id=46950ec797bb59105b0b7ec11153af89 (last visited: Jun. 10, 2023).

[Ser23e] ServiceNow, *ServiceNow Administration Fundamentals On Demand – On-Demand Course*, ServiceNow Learning Platform, 2023. [Online]. Available: https://nowlearning.servicenow.com/lxp?id=learning_course_prev&course_id=15788197875a995c24e0bb39dabb3503 (last visited: Jun. 10, 2023).

[Ser23f] ServiceNow, *Welcome to ServiceNow*, ServiceNow Learning Platform, 2023. [Online]. Available: https://nowlearning.servicenow.com/lxp?id=learning_course_prev&course_id=023708df1bc0119cf95e99b8bd4bcb76.

[TBDM14] S. Thalmann, D. Bachlechner, *et al.*, «Complexity is dead, long live complexity! How software can help service providers manage security and compliance», *Computers & Security*, vol. 45, pp. 172–185, Sep. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404814000935.

[Tho21] C. Thomas, *Risk Libraries - an Exiting New Future for Risk Management*, Jun. 2021. [Online]. Available: https://www.360factors.com/blog/risk-libraries-an-exciting-new-future-for-risk-management/ (last visited: Jul. 6, 2023).

[Wil93] T. M. Williams, «Risk-management infrastructures», *International Journal of Project Management*, vol. 11, no. 1, pp. 5–10, Feb. 1993. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0263786393900036.

[Wil94] T. M. Willams, «Using a risk register to integrate risk management in project definition», *International Journal of Project Management*, vol. 12, no. 1, pp. 17–22, Feb. 1994. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0263786394900051.

[WJ13] D. Watson and A. Jones, «Chapter 5 - Risk Management», in *Digital Forensics Processing and Procedures*, Boston: Syngress, Jan. 2013, pp. 109–176. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9781597497428000054.

[ZR08] G. A. Zsidisin and B. Ritchie, *Supply Chain Risk: A Handbook of Assessment, Management, and Performance*. Springer Science & Business Media, 2008.

Appendix A
Notification Form to Sikt

The following pages include the notification form which was sent to Sikt. The document is in Norwegian.

Sikt

Meldeskjema

Referansenummer
428478

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Beskriv hvilke bakgrunnsopplysninger du skal behandle

Arbeidssted, stilling.

Prosjektinformasjon

Prosjekttittel

Utilization of ServiceNow's Risk Management Functionality Within the GRC module: A Case Study

Prosjektbeskrivelse

Prosjektet er en masteroppgave i Kommunikasjonsteknologi og digital sikkerhet ved NTNU. Oppgaven skal utforske effektiviteten av å bruke GRC-modulen i plattformen ServiceNow for risikorapportering, og i hvilken grad et risikobibliotek kan bidra til å forbedre denne prosessen.
For å samle inn data, vil det gjennomføres intervjuer som tar sikte på å evaluere effekten av GRC-modulen på ulike aspekter som risikorapportering og beslutningsstøtte, og utforske utfordringer innen risikostyring. Intervjuobjektene vil bli spurt om samtykke til å ta opp lyd, og ved eventuelt samtykke vil lydopptak lagres. Andre persondata som er relevant er arbeidssted og stilling, i forbindelse med hvordan de forholder seg til risikorapportering og risikostyring på jobb.
Målet med prosjektet er å bidra til forståelsen av de potensielle fordelene og begrensningene ved å bruke ServiceNow og risikobiblioteker for risikostyring i organisasjoner, og om det kan håndtere identifiserte utfordringer.

Begrunn hvorfor det er nødvendig å behandle personopplysningene

Dybdeintervjuer med fagfolk vil være nødvendig for å samle inn et datagrunnlag til masteroppgaven. Temaet er ikke noe "mannen i gata" vil kunne svare på i en spørreundersøkelse, og dermed er bruken av intervju den hensiktsmessige formen for datainnsamling. Det vil ikke samles inn andre persondata enn det som er relevant til problemstillinn

Ekstern finansiering
Ikke utfyllt
Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Synne Bakke Kjærvik, synne.b.kjarvik@ntnu.no, tlf: 45076200

Behandlingsansvar

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Maria Bartnes, maria.bartnes@sintef.no, tlf: 45218102

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?
Nei

Utvalg 1

Beskriv utvalget

Personer som jobber med risikostyring og som jobber med ServiceNow plattformen.

Beskriv hvordan rekruttering eller trekking av utvalget skjer

Masteroppgaven skrives i samarbeid med ekstern bedrift, Sopra Steria. De vil bidra til å finne intervjuobjekter.

Alder
25 - 50

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

Hvordan samler du inn data fra utvalg 1?

Personlig intervju

Vedlegg

Intervjuguide.pdf

Grunnlag for å behandle alminnelige kategorier av personopplysninger
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av personopplysningene?
Ja

Hvordan?
Skriftlig informasjon (papir eller elektronisk)

Informasjonsskriv

Invitasjon til forskningsprosjekt.pdf

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?
Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

Ved å ta kontakt på mail eller telefon og si at de ønsker å trekke samtykket, så vil alle personopplysninger umiddelbart slettes

Hvordan kan de registrerte få innsyn, rettet eller slettet personopplysninger om seg selv?

Ved å ta kontakt på mail eller telefon, vil personene kunne få innsyn i sine personopplysninger, og få rettet eller slettet disse.

Totalt antall registrerte i prosjektet
1-99

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?
Ikke utfyllt

Behandling

Hvor behandles personopplysningene?

- Private enheter

Hvem behandler/har tilgang til personopplysningene?

- Prosjektansvarlig
- Student (studentprosjekt)
- Eksterne medarbeidere/samarbeidspartnere innenfor EU/EØS

Tilgjengeliggjøres personopplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?
Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?
Nei

Begrunn hvorfor personopplysningene oppbevares sammen med de øvrige opplysningene

Prosjektet er et studentarbeid, og jeg disponerer kun én (personlig) maskin til arbeidet.

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Andre sikkerhetstiltak

Hvilke

Automatisk lås på mobile enheter. Passordbeskyttelse på enhetene.

Varighet

Prosjektperiode
17.04.2023 - 07.07.2023

Hva skjer med dataene ved prosjektslutt?
Data slettes (sletter rådataene)

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?
Nei

Tilleggsopplysninger

Appendix B

Approval to Process Personal Data by Sikt

The following pages include the approval from Sikt. The document is in Norwegian.

Sikt

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
428478	Automatisk	17.03.2023

Prosjekttittel
Utilization of ServiceNow's Risk Management Functionality Within the GRC module: A Case Study

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Maria Bartnes

Student
Synne Bakke Kjærvik

Prosjektperiode
17.04.2023 - 07.07.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 07.07.2023.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)

- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

Appendix C

Invitation to Interview Participants

The following pages include the full invitation and information which was sent to the interview participants. The document is in Norwegian.

INVITASJON TIL Å DELTA I FORSKNINGSPROSJEKTET «Utilization of ServiceNow's Risk Management Functionality Within the GRC module: A Case Study»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å utforske effektiviteten av å bruke GRC-modulen i plattformen ServiceNow for risikostyring, og i hvilken grad et risikobibliotek kan bidra til å forbedre denne prosessen. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Intervjuet gjennomføres i forbindelse med masteroppgaven min i Kommunikasjonsteknologi og digital sikkerhet ved NTNU. Oppgaven tar sikte på å evaluere effekten av GRC-modulen på ulike aspekter som risikorapportering og beslutningsstøtte, og utforske utfordringer relatert til risikostyring. Målet med prosjektet er å bidra til forståelsen av de potensielle fordelene og begrensningene ved å bruke ServiceNow og risikobiblioteker for risikostyring i organisasjoner, og om det kan håndtere identifiserte utfordringer.

NTNU er ansvarlig for prosjektet. Oppgaven skrives i samarbeid med ekstern bedrift, Sopra Steria, som har bidratt med å finne intervjuobjekter.

Hvis du velger å delta i prosjektet, innebærer det å delta på et dybdeintervju. Det vil ta deg ca. 1 time, og intervjuet vil handle om risikostyring, risikorapportering, utfordringer relatert til dette, bruken av ServiceNow og bruken av risikobiblioteker.

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Intervjuene vil brukes som datagrunnlag i masteroppgaven, og vil analyseres for å prøve besvare problemstillingen. Ved eventuelt samtykke til det, vil det bli tatt lydopptak av intervjuet. Dataene vil ikke brukes på en måte som kan identifisere intervjuobjektet, og vil slettes etter endt prosjekt i juli. All data vil oppbevares på passordbeskyttet maskin, og bare student og veileder vil ha innsyn i dem. Ved å ta kontakt med meg eller veileder på e-post eller telefon vil man kunne få innsyn i hvilke opplysninger som er samlet inn, få endret disse eller slettet de.

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- NTNU ved Maria Bartnes, epost: maria.bartnes@sintef.no eller telefon: 452 18 102.
- Vårt personvernombud: Thomas Helgesen, epost: thomas.helgesen@ntnu.no eller telefon: 930 79 038.

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen

Maria Bartnes

(Veileder)

Synne Bakke Kjærvik

(Student)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet «Utilization of the ServiceNow GRC Module: A Case Study» og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju
- ☐ at intervjuer kan ta opp lyd

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet.

(Signert av prosjektdeltaker, dato)

Appendix D
Interview Guide

The following pages include the interview guide used in the semi-structured interviews. The guide is in Norwegian.

INTERVJUMAL "Utilization of ServiceNow's Risk Management Functionality Within the GRC module: A Case Study"

Q: Hva er din stillingstittel i organisasjonen din?

A:

Q: Hva er dine erfaringer med risikostyring i organisasjonen din?

A:

Q: Hva er de største utfordringene dere har opplevd når det gjelder risikostyring i organisasjonen, og hvordan har dere prøvd å håndtere disse utfordringene?

A:

Q: Hvordan vil du beskrive organisasjonens risikokultur, og hva slags tiltak kan gjøres for å forbedre denne kulturen?

A:

Q: Hvordan kan organisasjonen din sørge for at risikostyring blir en del av daglig drift og ikke bare en sjekkliste som følges før rapportering?

A:

Q: Har organisasjonen din erfaring med bruk av ServiceNow-plattformen for risikostyring og GRC-modulen? Hvis ja, hva er din vurdering av disse verktøyene?

A:

Q: Hvis nei, hvilke verktøy bruker dere for å identifisere og håndtere potensielle risikoer i organisasjonen, og hvordan fungerer disse verktøyene?

A:

Q: Hvordan ble risikostyring organisert i organisasjonen din før dere implementerte ServiceNow's GRC-modul og risikobiblioteket?

A:

Q: Hva var de største utfordringene dere møtte med den tidligere metoden for risikostyring?

A:

Q: Hva var hovedårsaken(e) til at organisasjonen din valgte å implementere ServiceNow's GRC-modul for risikostyring?

A:

Q: Har organisasjonen din opplevd utfordringen med å få et helhetlig bilde av risikolandskapet? Tror du GRC-modulen i ServiceNow kan bidra til å løse dette problemet?

A:

Q: Hvordan har overgangen fra den tidligere metoden til bruk av ServiceNow's GRC-modul påvirket organisasjonens risikostyringskultur?

A:

Q: Har dere opplevd noen utfordringer eller begrensninger ved implementering og bruk av GRC-modulen i ServiceNow? Hvordan har dere håndtert disse?

A:

Q: Hvordan påvirker organisasjonens størrelse og struktur bruk og implementering av ServiceNow's GRC-modul og risikobiblioteket?

A:

Q: Har det vært noen utfordringer med å tilpasse ServiceNow's GRC-modul til organisasjonens spesifikke behov og kontekst?

A:

Q: Har det vært noen utfordringer med å integrere ServiceNow's GRC-modul med andre systemer eller prosesser i organisasjonen din?

A:

Q: Hva er fordelene dere har sett med å bruke GRC-modulen i ServiceNow for risikostyring?

A:

Q: Hvordan kan GRC-modulen i ServiceNow hjelpe organisasjonen din med å bedre håndtere risikoer og forbedre rapporteringen av disse risikoene?

A:

Q: Hvordan kan GRC-modulen i ServiceNow bidra til å styrke organisasjonens etterlevelse av gjeldende reguleringer og standarder?

A:

Q: Hvordan kan GRC-modulen i ServiceNow hjelpe organisasjonen din med å overvåke risikoen over tid, og hva slags funksjoner tror du er spesielt viktige i denne sammenhengen?

A:

Q: Hvis du kunne endret noe ved ServiceNow's GRC-modul for å forbedre organisasjonens risikostyringsprosess, hva ville det være?

A:

Q: Bruker organisasjonen din et risikobibliotek i forbindelse med risikostyring? Hvis ja, hvordan har det bidratt til å forbedre prosessen?

A:

Q: Hva er dine forventninger til bruk av et risikobibliotek i organisasjonen, og hvordan tror du det kan bidra til en mer effektiv risikostyring?

A:

Q: Hvordan kan et risikobibliotek hjelpe organisasjonen din med å identifisere og vurdere risikoer i ulike forretningsområder og funksjoner?

A:

Q: Hvordan håndterer organisasjonen forskjeller i risikooppfatning blant forskjellige grupper av ansatte, og hvordan bidrar ServiceNow's GRC-modul og risikobiblioteket i dette?

A:

Q: Har bruk av ServiceNow's GRC-modul og risikobiblioteket hjulpet organisasjonen din med å identifisere nye risikoer, eller har det endret hvordan dere prioriterer eksisterende risikoer?

A:

Q: Er det noen spesifikke tilfeller hvor ServiceNow's GRC-modul og risikobiblioteket har hjulpet dere med å identifisere og håndtere en risiko som dere kanskje ikke ville oppdaget eller håndtert effektivt uten disse verktøyene?

A:

Q: Hvordan påvirker ServiceNow's GRC-modul organisasjonens evne til å reagere på og håndtere identifiserte risikoer?

A:

Q: Hvordan involverer organisasjonen forskjellige avdelinger og ansatte i risikostyringsprosessen, og hvordan støtter ServiceNow's GRC-modul og risikobiblioteket denne involveringen?

A:

Q: Hvordan har organisasjonen din håndtert opplæring og opplæringsbehov relatert til bruk av ServiceNow's GRC-modul og risikobiblioteket?

A:

Q: Har bruk av ServiceNow's GRC-modul og risikobiblioteket bidratt til å redusere feil og inkonsekvenser i risikostyringsprosessen?

A:

Q: Hvordan blir resultatene fra risikovurderinger formidlet til relevante interessenter i organisasjonen din, og har ServiceNow's GRC-modul bidratt til å forbedre denne prosessen?

A:

Q: Hvordan vurderer organisasjonen din effekten av tiltakene som er implementert for å håndtere risikoer, og i hvilken grad bidrar ServiceNow's GRC-modul og risikobiblioteket i denne prosessen?

A:

Q: Har bruk av ServiceNow's GRC-modul og risikobiblioteket endret organisasjonens tilnærming til risikostyring? Hvis ja, hvordan?

A:

Q: Hvordan har organisasjonens interne og eksterne kommunikasjon om risikostyring endret seg siden implementeringen av ServiceNow's GRC-modul og risikobiblioteket?

A:

Q: Hvordan har bruk av ServiceNow's GRC-modul og risikobiblioteket bidratt til å oppfylle organisasjonens overordnede mål og strategier?

A:

Q: Hvilke andre mulige forbedringer tror du organisasjonen din kan oppnå ved å bruke GRC-modulen i ServiceNow og risikobiblioteket for risikostyring?

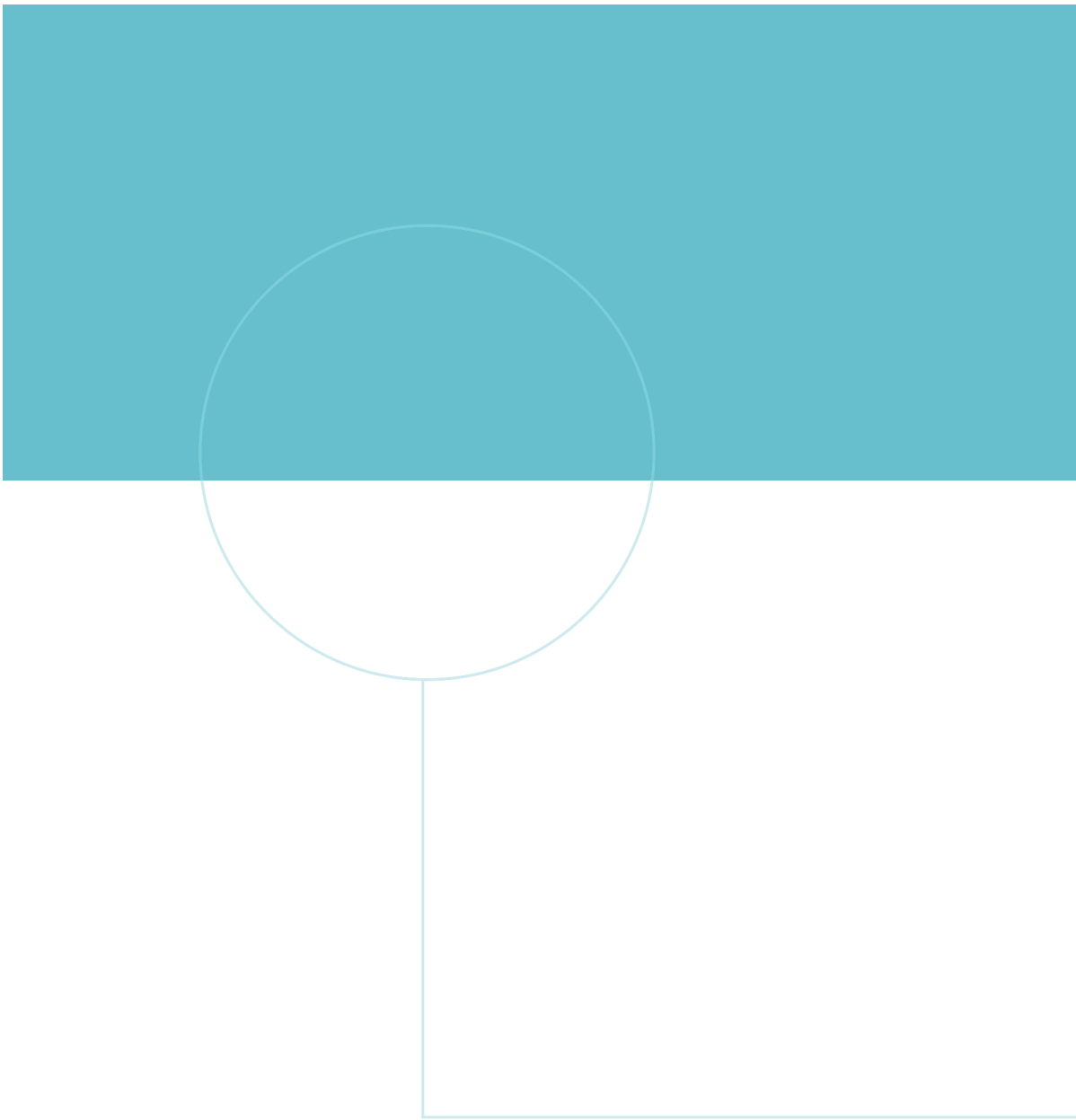
A:

Q: Hva er dine forventninger til fremtidig utvikling og bruk av ServiceNow's GRC-modul og risikobiblioteket i organisasjonen din?

A:

Q: Har du noe annet du vil legge til?

A:



NTNU

Norwegian University of
Science and Technology