Unveiling Shadows: A framework for identifying, assessing, and mitigating risks associated with Shadow IT

Master thesis
Master of Information Management
Tilburg School of Economics and Management
Tilburg University

University supervisor: M. Struijk
Second reader: C. Ou
Company supervisor: Y. Sufta
Internship company: EY

7 June 2023

Management summary

The growth of information technology (IT) services has been accelerated by the COVID-19 pandemic, which has stimulated remote work capabilities. Consequently, this is also tied to the rise of Shadow IT (SIT), which poses a growing threat to organizations due to its hidden nature characterized by the unauthorized usage of IT tools by employees. Organizations are struggling with this risk because it can lead to compliance issues, data loss, and lack of visibility and control. Existing risk management frameworks do not fully answer those risks, and this leaves room for addressing that need for control.

This research aims to develop a practical IT risk management framework for identifying, assessing, and managing SIT risks within organizations. The following main research question is formulated: *"How can an IT risk framework be successfully developed to effectively identify, assess and manage SIT risks within organizations?".* The research follows a design science research approach, consisting of an extensive literature review to understand the characteristics of SIT. In addition, semi-structured individual interviews with experts were conducted to develop and validate the SIT risk management framework.

The developed risk management framework is based on existing IT risk management frameworks such as COBIT, ISO/IEC, and NIST, and it incorporates specific solutions to address the unique challenges of SIT. The findings of the research determined that the framework should consist of four phases: "Prevent", "Identify", "Assess", and "Respond", each phase managing the different aspects of SIT. The "Prevent" phase proactively averts the emergence of SIT determinants. This is achieved by the implementation of tasks that relate to governance and information security. Following the "Prevent" phase, the "Identify" phase begins and focuses on enabling organizations to identify unknown IT assets present in their infrastructure. This process relies heavily on asset management activities to detect the various types of SIT instances. Subsequently, the "Assess" phase involves evaluating the risk impact, compliance, analyzing user behavior, and identifying alternative tools to mitigate the different SIT risks. The mitigation tasks in this phase correspond to risk categorization, user understanding, and data management. Finally, the "Respond" phase encompasses the planning and action tasks to manage and mitigate the identified SIT instance based on the information retrieved from earlier phases. The framework is designed to provide a holistic and practical approach for organizations to mitigate SIT risks. However, research findings reveal many companies lack adequate resources and time to effectively detect and address SIT instances. Participants in the study emphasized that organizations often overlook SIT as a security priority. This highlights the urgent need for organizations to prioritize SIT within their agendas, as only then will they be inclined to allocate the necessary resources to implement a comprehensive framework for detecting and managing Shadow IT instances.

This research enhances the current academic and managerial understanding of managing SIT risks by developing a practical framework. It stands as one of the few empirical studies that aims to address SIT risks systematically. The framework extends the existing identification and evaluation steps of SIT, as previously explored by Rentrop and Zimmermann (2012a). It incorporates mitigation tasks for SIT determinants, SIT risks, and SIT types as it integrates these aspects into a comprehensive IT risk management framework. Furthermore, this research contributes to existing IT risk management frameworks, addressing the challenge of practical implementation highlighted by Tøndel et al. (2014). Participants in the study noted the ease of interpretability of the framework as it provides practical guidance for organizations in managing SIT risks. While the framework has garnered positive feedback from experts, further validation and refinement are necessary to evaluate its effectiveness in real-world scenarios.

Acknowledgements

This research paper serves as the culmination of my journey through the MSc Information Management program at Tilburg University. This thesis was written between January 2023 and June 2023, during an internship at EY a professional service organization. It is with great pleasure and gratitude that I take this opportunity to acknowledge and express my appreciation to the individuals and organizations who have contributed to the successful completion of this work.

I would like to thank the teachers at Tilburg University for sharing their knowledge and dedication towards educational excellence. The courses that I undertook were insightful and contributed towards my knowledge in this field of study. I am thankful towards my university supervisor Mylène Struijk for her support, expertise, and guidance during my research. The research capabilities that I gained during this period are held dear to my heart and I hope to leverage this in my professional career.

Moreover, I would like to extend my gratitude towards EY for this research opportunity to conduct it at their organization. I am thankful for the colleagues who have helped me during this period for their knowledge and enthusiasm. Lastly, I would like to thank my family, girlfriend, and friends, who have supported me during this academic journey.

Kevin Huang

List of contents

List of figures

List of tables

List of acronyms

APO	Align, Plan and Organize
BIO	Baseline Informatiebeveiliging Overheid
BUs	Business Units
BYO	Bring Your Own
CIOs	Chief Information Officers
CIS	Center for Information Security
COBIT	Control Objectives for Information and Related Technologies
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
IoT	Internet of Things
IS	Information Systems
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
SaaS	Software as a Service
SIT	Shadow Information Technology
SP	Special Publication

1. Introduction

This chapter outlines the problem indication as the first section, the next section states the problem statement, Section 1.3 provides the research questions surrounding the topic, Section 1.4 explains the research method during this study, Section 1.4 and Section 1.5 provides the general structure of the research.

1.1. Problem indication

In the past years, the IT industry has risen significantly, and this was accelerated by the lockdown period during the COVID-19 pandemic. It is estimated that the usage of internet services, systems and networks increased from 40% to 100% since pre-COVID times as employees were forced to work from home (De' et al., 2020). It is further predicted that the same trend will continue in the foreseeable future in the same manner as during the lockdown. The usage of SIT has also increased by 59% since the start of the pandemic (Core, 2021). This is likely due to the usage of the number of cloud services, as it has increased by 22% in early 2021, and 97% of cloud applications are determined to be SIT instances (Netskope Threat Labs, 2021).

SIT (also known as rogue IT, feral systems, shadow systems, or workaround systems) refers to hardware, software, or services developed and/or used for the job without awareness, approval, knowledge, or support of the IT department (Haag & Eckhardt, 2017; Silic & Back, 2014). It can include everything from employees using unapproved personal devices and apps for work-related tasks to entire departments using software that has not been vetted by the IT team. The notable organizational information security risks associated with SIT are “compliance issues, wasted time, inconsistent business logic, increased risks for data loss or leaks and wasted investment” (Silic & Back, 2014, p. 274). Additionally, the lack of visibility and control that comes with SIT can make it difficult for IT teams to manage and maintain the organization's technology infrastructure (Behrens, 2009).

The number of cybersecurity attacks has seen a 50.1% increase since the pandemic and highlighted that the control of information is of strategic importance due to the increased number of cyber-attacks on information systems (IS) (Lallie et al., 2021). The average cost of a data breach in 2022 costs $4.35 million (IBM, 2023) and security experts predicted that by 2025 worldwide cybercrime costs are up to $30 billion annually (Cybersecurity Ventures, 2022). In 2019, Microsoft conducted a security assessment on a sample of known SIT applications and concluded that all tested applications failed to meet at least two out of three key security requirements (Inside Track Staff, 2023). Moreover, in the past year, seven out of ten organizations have been compromised by the usage of SIT (Randori, 2023).

1.2. Problem statement

It can be stated that SIT can be utilized by both individuals and groups, and it has seen a growth in usage due to recent trends such as Bring Your Own (BYO) policies, cloud computing, and IT consumerization (Kopper & Westner, 2016b). SIT introduces internal threats for organizations with volitional but non-malicious intention to violate an organization’s IS security and IT policy (Haag & Eckhardt, 2014). The potential risks an organization could face due to SIT are data loss, IT security, system inefficiencies, and financial costs (Silic et al., 2016). In terms of financial costs, industry experts from Gartner have estimated that 30 to 40% of IT spending in large enterprises takes place outside of the IT department, and Everest Group indicates that the number is likely 50% or more (Bendor-Samuel, 2017).

Insider threats are listed as the top security threat challenge that organizations must deal with and is among researchers and professionals deemed as one of the most difficult challenges to handle (Silic et al., 2017). This is further outlined by a recent Software as a Service (SaaS) report that surveyed 300 IT leaders, and 60% stated that they are not aware of what cloud applications are used by employees within their organization (Torii, 2022). The report also states that only 20% of IT leaders work often or continuously with security and/or compliance teams to help discover and mitigate the risks of SIT. In the organizational context, there is a lack of awareness of managing SIT, as 60% of organizations do not include SIT in their threat assessment (Cisco Umbrella, 2021).

Organizations have adopted management frameworks such as ISO/IEC, COBIT and ITIL that facilitate prevention and detection as a response to potential security incidents (Cram et al., 2017). However, management and security policies following from those frameworks lose their efficacy when users do not comply with such measures (Puhakainen & Siponen, 2010). This is especially true to SIT as it is hard to detect SIT instances with existing policies because those systems are well hidden (Kopper et al., 2020). Moreover, existing management and security frameworks such as COBIT and ITIL do not offer specific solutions to deal with SIT (Ozkan et al., 2021; Rentrop & Zimmermann, 2012a; Šedivcová & Potančok, 2019). It is explained that the ITIL framework is not inherently designed as a security standard as it focuses more on IT service management and delivery (Peltier, 2017). Due to the lack of guidelines, organizations cannot perform holistic assessments of risks and architectural factors regarding SIT (Zimmermann et al., 2017). It is further noted that current research does not comprehend the full scope of the utilization of SIT by employees in the organizational context (Silic & Back, 2014).

SIT increases the likelihood of unofficial data flows that cause compliance issues with existing frameworks and regulations such as COBIT, ITIL, GDPR, and the Sarbanes-Oxley Act because SIT has no scope for proper documentation and approval (Reddy, 2021; SoftwareOne, 2023). Due to its non-compliant nature, SIT poses a serious financial, legal, and reputational threat to organizations (Györy et al., 2012). Organizations and individuals can face hefty fines or even jail time when they are non-compliant with those regulations (Garbutt, 2022). For instance, severe violations of organizations with GDPR regulations include fines of up to 20 million euros or even up to 4 percent of an organization’s total global turnover (GDPR, 2016).

It is stressed that a consistent approach needs yet to be developed at organizations to successfully identify and deal with SIT to create transparency, increase maturity of processes and enable IT control (Rentrop & Zimmermann, 2012a). The topic of managing SIT in both the academic and professional world is barely explored and existing frameworks are underdeveloped in managing the risks of SIT. As stated from earlier sources, if SIT is left uncontrolled organizations cannot apply the necessary risk measures, audit the unauthorized instances, or document compliance, and cannot identify all the details if a data breach occurs (Garbutt, 2022). This research is conducted at EY a professional services firm, who is interested in a security framework that can effectively mitigate and manage the risks of SIT.

1.3. Research questions

The above-mentioned problem statement has resulted in the following research question and its supported sub-questions. The following main research question has been formulated: *“How can an IT risk framework be successfully developed to effectively identify, assess and manage SIT risks within organizations?”*. Table 1 indicates the sub-questions that help answer the main research question.

Table 1. Sub-questions and description

Nr.	Sub-questions	Description
1	What are the characteristics of SIT?	This question aims to understand the phenomenon and provides the context for the development of the framework.
2	What are the current available methods and frameworks that address SIT?	This question will identify the existing methods and frameworks that address SIT as a risk and vulnerability in organizations. The existing frameworks will be analyzed, compared, and used as a foundation for the research.
3	What are the requirements of risk management experts to develop a SIT risk management framework?	This question will identify the requirements by experts in the industry to fill the gaps in existing frameworks to develop a SIT risk management framework.
4	To what extent can the SIT risk management framework be utilized by organizations?	This question will address if the developed SIT risk management framework is feasible to use in real-world applications and whether the framework applies to every scenario or if it needs any adjustments.

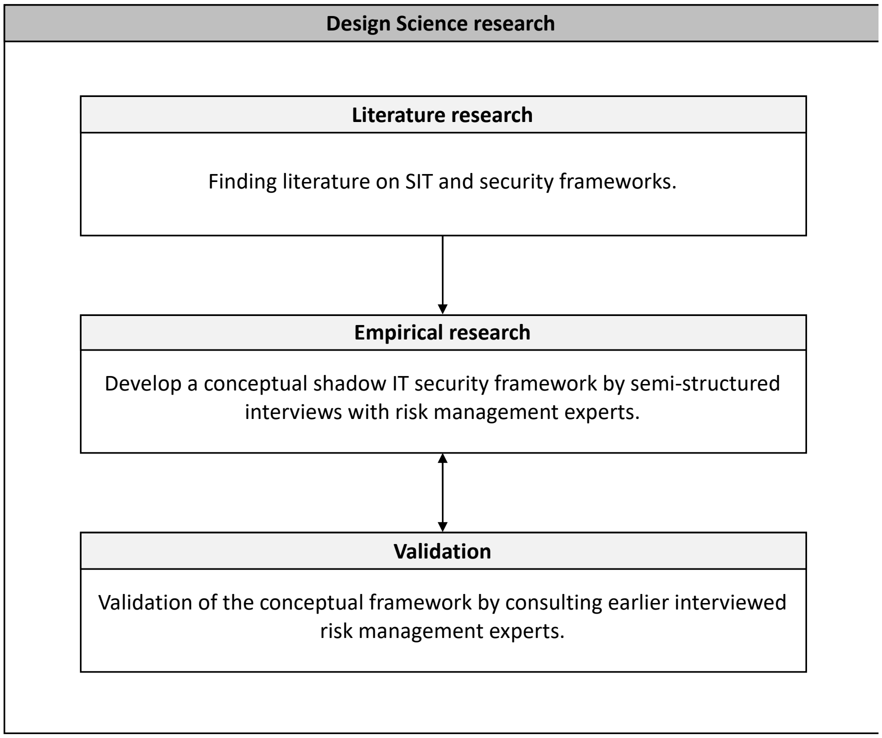
1.4. Research method

The research performed is a design science research approach and consists of theoretical research and empirical research. First, theoretical research is conducted with a literature review that searches for academic literature to obtain current knowledge on the topic. The literature review will be conducted by the method of Wolfswinkel et al. (2013). Although the method is designed for a grounded theory approach, the structured method is useful to evaluate existing literature as it consists of a rigorous five step approach in reviewing sources that can also be applied to design science research. Second, empirical research is conducted to further design, develop, and evaluate the artifact (Hevner et al., 2004). The design science problem is visualized to help design the artifact (Wieringa, 2014) and this can be seen below in Table 2.

Table 2. Design science problem (Wieringa, 2014)

Design science problem	
Improve	< information security >
By	< developing a framework >
That satisfies	< the management of SIT risks >
In order to	< effectively help and consult organizations >

The empirical research is conducted with semi-structured individual interviews to develop the initial conceptual framework. The final framework will then be evaluated and validated by individuals who were interviewed earlier. The participants for the interviews are experts who are knowledgeable of SIT and risk management. The validation interviews are held in two rounds, as the framework will be validated twice. The overall structure of the research can be seen in Figure 1.



Finding literature on SIT and security frameworks.

Develop a conceptual shadow IT security framework by semi-structured interviews with risk management experts.

Validation of the conceptual framework by consulting earlier interviewed risk management experts.

Figure 1. Research structure

1.5. Thesis structure

The overview of the research is structured as follows: an extensive literature review is conducted. Thereafter, the research method is presented and followed by gathering the results and the design and validation of the artefact. Subsequently, the results are discussed. Finally, the conclusion is given, where the main question and sub-questions are answered.

2. Literature review

This chapter discusses literature research for understanding the main topic of this research. It is necessary to get familiar with the literature landscape to design and develop a reliable and valid artifact. During the literature research important aspects of SIT and existing management frameworks are explored to develop a deeper understanding. The research methods used during the literature review can be found in Appendix A.

The first section introduces SIT. Section 2.2 provides the distinction between the types of SIT. Section 2.3 elaborates the determinants of SIT. Section 2.4 explains the effects of SIT. Lastly, Section 2.5 discusses the risk management of existing frameworks to address SIT.

2.1. Introduction to SIT

SIT, alternatively referred to as rogue IT, feral systems, shadow systems, or workaround systems, encompasses hardware, software, or services that are constructed, introduced, and/or employed for job-related purposes without obtaining explicit approval or knowledge from the organization (Haag & Eckhardt, 2017; Silic & Back, 2014). The phenomenon of SIT is recognized as a security concern, specifically an "insider threat" in which a well-intentioned individual (i.e., employee) installs unapproved software and engages in non-compliant behavior regarding information security policies (Györy et al., 2012; Silic & Back, 2014). Consequently, Chief Information Officers (CIOs) are experiencing a growing loss of control over the IT landscape within organizations, resulting in heightened risks to IS security posed by SIT (Silic & Back, 2014). Moreover, as SIT fosters the proliferation of dispersed and potentially unknown enterprise data sources, the accuracy and reliability of decisions based on (big) data analytics diminish (Fürstenau & Rothe, 2014; Haag & Eckhardt, 2017). To tackle this challenge, it is imperative for CIOs and IT managers to acquire a better understanding of the underlying mechanisms, causes, and consequences of SIT (Haag & Eckhardt, 2017).

The different concepts of personal IT, target IT, IT consumerization, and workaround systems are closely related to SIT. However, each concept has its own characteristics that set them apart from SIT. Personal IT describes the use of personal devices in an organizational setting, where privately owned hardware intended for the consumer market is also used for business purposes (Afreen, 2017). The concept of target IT is provided by the organization to perform IT-supported work tasks, and it can be either centralized IT or decentralized IT, depending on whether it is controlled by the BUs or IT department (Haag & Eckhardt, 2017). The trend of IT consumerization is the adoption of consumer devices, applications, and services in the workforce driven by changing practices and expectations of employees that influences IT-related activities (Gregory et al., 2018). Organizational IT policies have been set up to use target IT and personal IT appropriately. This includes rules, guidelines, standards, and procedures with the intent to restrict undesired use (Liang et al., 2013). However, organizational IT policies are circumvented when users are hindered from their task performance and this leads to the usage of workaround systems (Alter, 2014; Haag & Eckhardt, 2017).

IT consumerization plays a role in all stages of IT-related activities, and such instances include the use of target IT, personal IT, SIT, and non-IT (Haag & Eckhardt, 2017). A workaround system is a goal-driven adaptation to an existing work system to overcome structural constraints from existing work systems that would normally prevent users from achieving organizational goals (Alter, 2014). Workaround systems include modifications of personal IT, target IT or the usage of SIT, where employees use unmanaged applications or devices that store business information to achieve the necessary business goals (Walters, 2013). Employees can also adopt a non-IT workaround without the use of IT, such as collecting data or processing information on paper (Haag & Eckhardt, 2017). Figure 2 illustrates the differentiation between SIT, IT consumerization, workaround systems, and other closely related concepts.

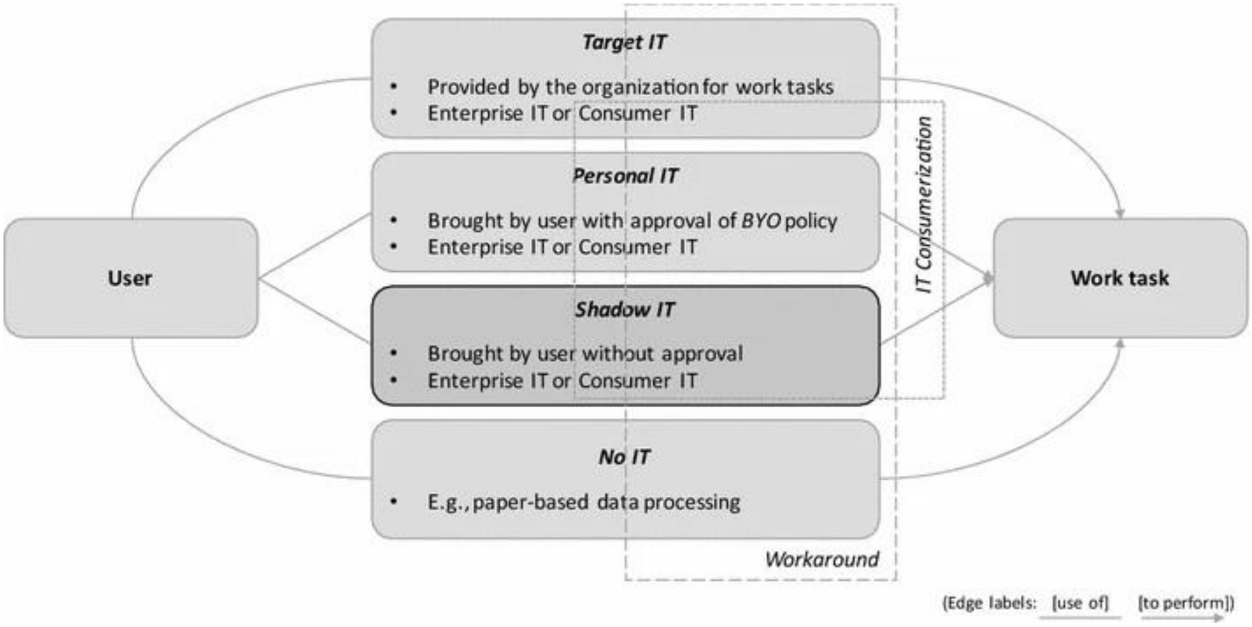
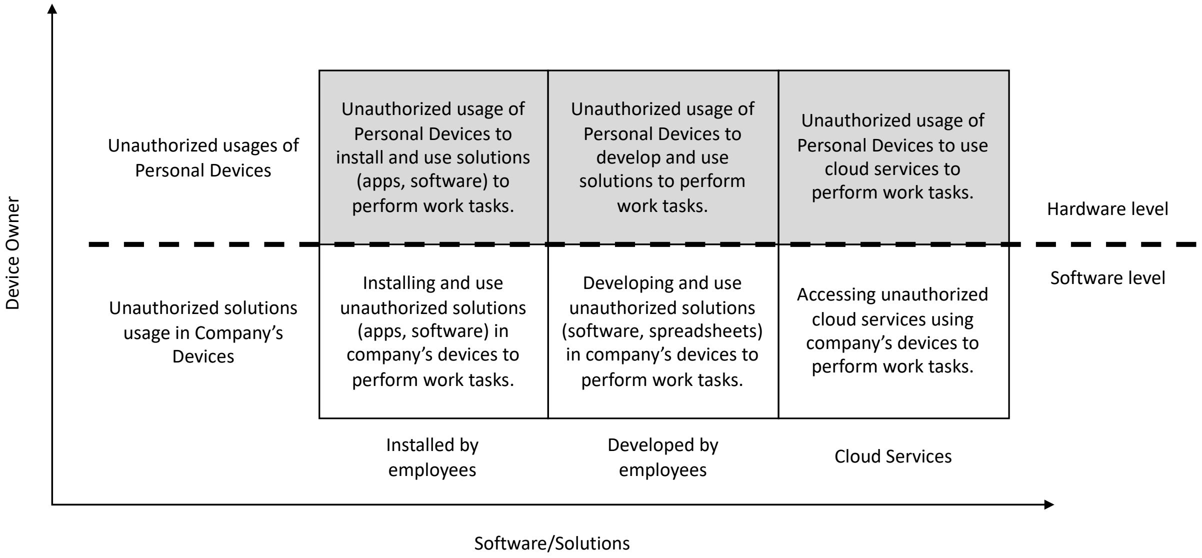

User
Target IT
Provided by the organization for work tasks
Enterprise IT or Consumer IT
Personal IT
Brought by user with approval of BYO policy
Enterprise IT or Consumer IT
Shadow IT
Brought by user without approval
Enterprise IT or Consumer IT
No IT
E.g., paper-based data processing
IT Consumerization
Workaround
Work task
(Edge labels: [use of] [to perform])

Figure 2. SIT and other closely related concepts (Haag & Eckhardt, 2017, p. 470).

2.2. SIT types

Individual users, workgroups, or whole BUs can use SIT as a form of decentralized computing to perform work tasks (Fürstenau et al., 2017). These work tasks circumvent existing compliance standards, such as the use of unapproved cloud services or manipulating spreadsheets (Zimmermann et al., 2017). There exist four types of SIT usage, namely unauthorized cloud services, self-made solutions, self-installed applications, and the use of personal devices (Mallmann et al., 2018). In the first instance, unauthorized cloud services represent the accessed software through the internet and do not need to be installed on the device (Fürstenau & Rothe, 2014; Walterbusch et al., 2017). Second, self-made solutions are solutions developed and used by employees on the company's IT assets to perform their work tasks, this can vary from a simple spreadsheet for a single user to a complex software application to be used by a whole BU (Zimmermann et al., 2017). Thirdly, self-installed applications include solutions that are freely available, installed, and used by employees on the company's devices (Jones et al., 2004; Silic & Back, 2014). Finally, self-acquired devices represent the hardware used by SIT, this includes devices personally purchased and owned by the employees instead of the organization, which includes the use of applications in the personal devices at the workplace (Zimmermann et al., 2017). Figure 3 illustrates how the four SIT types can occur within organizations.



	Installed by employees	Developed by employees	Cloud Services	
Unauthorized usages of Personal Devices	Unauthorized usage of Personal Devices to install and use solutions (apps, software) to perform work tasks.	Unauthorized usage of Personal Devices to develop and use solutions to perform work tasks.	Unauthorized usage of Personal Devices to use cloud services to perform work tasks.	Hardware level
Unauthorized solutions usage in Company's Devices	Installing and use unauthorized solutions (apps, software) in company's devices to perform work tasks.	Developing and use unauthorized solutions (software, spreadsheets) in company's devices to perform work tasks.	Accessing unauthorized cloud services using company's devices to perform work tasks.	Software level

Figure 3. The occurrences of SIT (Mallmann et al., 2018, p. 20).

2.3. Determinants of SIT

Organizational systems are implemented to increase standardization and control, but end-users create workarounds in the form of SIT because of inflexibility, unreliability, and lack of coordination (Raković et al., 2020). Employee dissatisfaction with the existing organizational systems provides breeding ground for the development of SIT (Kerr & Houghton, 2010). Three categories can be distinguished from determinants of SIT: (1) enablers, (2) motivators, and (3) missing barriers (Klotz et al., 2019). The following paragraph elaborates on the three categories.

2.3.1. Enablers

Technical accessibility

Technical accessibility is increasing as IT complexity decreases and technology offerings expand (Klotz et al., 2019). It becomes easier for business units (BUs) to deploy them autonomously (Spierings et al., 2017), since IT solutions become more user-friendly (Fernely, 2007; Silic & Back, 2014). In this evolution, Web services and solutions play a significant role (Jones et al., 2004). In addition, cloud services offer simpler application distribution models (Klotz et al., 2019; Walterbusch et al., 2017). Since employees use cloud services in their daily private life, it is probable that they also use the known benefits in their work (Walterbusch et al., 2017; Zimmermann & Rentrop, 2014).

IT user competence

IT knowledge availability is increasing in BUs (Spierings et al., 2017), leading BUs to build or acquire IT solutions independently without involving the IT department, reinforcing the emergence of SIT (Chua et al., 2014; Klotz et al., 2019; Kopper & Westner, 2016a). This is especially true for people who have grown up with IT and use it daily in their lives, as they can easily create and utilize IT solutions (Davison & Ou, 2018; Rentrop & Zimmermann, 2012b).

2.3.2. Motivators

Poor business-IT alignment

IT departments lack business knowledge and are often more focused on their internal goals (Fürstenau et al., 2017). The lack of communication between business and IT departments is further deepening this divide (Beimborn & Palitza, 2013). In addition, researchers indicate that the business processes are not sufficiently supported (Röder et al., 2014; Tambo & Bækgaard, 2013) and are often not transparent, which leads to unmatched expectations (Behrens & Sedera, 2004). For instance, a high level of formalization of processes with extensive documentation requirements can lead to misunderstanding (Buchwald & Urbach, 2012). A low level of trust is created between the business and the IT departments over time since both departments can develop negative experiences with each other (Silic & Back, 2014; Silic et al., 2016).

Shortcomings of IT systems

One of the motivations for SIT is caused by the lack of features in existing systems (Klotz et al., 2019; Zimmermann et al., 2017), which leads to not meeting the users' requirements (Behrens & Sedera, 2004; Boudreau & Robey, 2005; Kerr et al., 2007; Lyytinen & Newman, 2015). For instance, formal IT systems may be perceived as highly standardized, complex, and inflexible (Boudreau & Robey, 2005; Houghton & Kerr, 2006; Huuskonen & Vakkari, 2013) and therefore inadequate for processes such as enabling employee communication (Klotz et al., 2019). A poor alignment of the system with local needs, leading to a consequent loss of productivity (Kopper and Westner, 2016a). Hence, there is a gap between the offered IT systems and the users' requirements (Spierings et al., 2017; Zimmermann & Rentrop, 2014), leading users to develop SIT solutions as an alternative because of their easy adaptability (Kopper & Westner, 2016a).

2.3.3. Missing barriers

Misalignment of IT governance

Missing or too strong technical IT restriction policies and guidelines in organizations are one of the influencing factors leading to SIT. The implementation of IT restrictions policies would have limited effects in driving users away from SIT (Haag, 2015; Kopper & Westner, 2016a). These restrictions can be seen as an obstacle for innovation and functions as a cause for SIT (Walterbusch et al., 2017). The reasons for non-compliance are that employees either do not see the advantage or do not agree with the organization's existing guidelines (Behrens, 2009).

Lack of awareness

In general, employees are not aware of the existing IT policies. Even if employees are aware that IT policies do exist, they usually do not know the specific contents that are outlined (Klotz et al., 2019). In addition, employees are not aware of the potential impact of SIT, such as with respect to violating a regulation (Haag et al., 2015; Klotz et al., 2019). In some cases, employee training on IT policies has been removed for cost considerations (Walterbusch et al., 2017).

2.4. Effects of SIT

SIT possesses a significant dual-use context, where its utilization can yield both positive and negative effects (Silic & Back, 2014). Regarding potential positive effects, SIT systems can demonstrate high efficiency and effectiveness as alternatives to existing formal and standardized systems (Behrens & Sedera, 2004). On the other side, negative effects are existing risk of undermining the official system and even causing harm to organizational data and processes (Silic & Back, 2014). This section elaborates on the positive and negative effects of SIT.

2.4.1. Positive effects

Productivity gain

The adoption of SIT can bring about benefits for organizations, such as increased productivity (Zimmermann et al., 2017), efficiency (Röder et al., 2014), and effectiveness (Walterbusch et al., 2017). This is largely attributed to the improvement in individual employee performance that can be achieved by using SIT (Györy et al., 2012; Haag et al., 2015). As a result, workflows are enhanced, and business processes are better supported (Jones et al., 2004; Klotz et al., 2019). Additionally, users tend to perform better when utilizing self-developed solutions as opposed to solutions developed by others (Klotz et al., 2019).

Innovation

Interacting with different types of SIT can enhance an organization's technological innovation capabilities (Behrens, 2009; Klotz et al., 2019). Staying up to date with the constant developments in the fast-paced IT industry is challenging but less demanding when initiatives from all employees of the organization are acknowledged (Behrens, 2009; Györy et al., 2012).

User satisfaction

Employees tend to favor SIT, which can result in greater user satisfaction due to the availability of specific functionalities or familiarity with the technology. In addition, self-developed applications are often perceived by users as having superior quality, leading to improved decision-making performance (Klotz et al.,2019). Moreover, SIT offers higher flexibility (Behrens, 2009; Huber et al., 2017) due to their adaptability (Zimmermann et al., 2014).

2.4.2. Negative effects

Security risks

The potential loss of data or information leakage are security risks that are frequently highlighted as one of the most well-known negative effects of SIT (Kopper & Westner, 2016a; Silic & Back, 2014). This underscores the importance of addressing privacy concerns, particularly when managing highly sensitive personal information (Huuskonen & Vakkari, 2013).

Integration risks & data inconsistency

SIT frequently lacks integration with authorized systems (Azad & King, 2012), may depend on suboptimal architectural principles (Fürstenau et al., 2017), and is not standardized (Györy et al., 2012; Klotz et al., 2019). Loose coupling or a low degree of integration can result in data inconsistency, which is considered one of the greatest risks associated with SIT (Berente et al., 2008; Kopper & Westner, 2016a). Additionally, the adoption of SIT solutions may result in data inconsistencies (Walterbusch et al., 2017) or errors (Klotz et al., 2019; Myers et al., 2017).

Control loss

SIT can lead to a loss of control in assets as systems operate outside established structures (Behrens, 2009; Kopper & Westner, 2016a), causing disruption to the controlled organizational environment (Györy et al., 2012; Tambo & Bækgaard, 2013). This results in a lack of compliance with management objectives and organizational goals (Klotz et al., 2019; Röder et al., 2014). An example of this is the loss of control over data that can occur due to SIT (Walters, 2013). In addition, the loss of control over data and security can also cause regulatory compliance breaches, whereas following the GDPR an organization must provide an adequate level of security of the processing and managing of corporate and individual data and if a breach occurs that it needs to provide incident logs within 72 hours (Krystlik, 2017).

Synergy loss & inefficiency

The loss of potential synergies due to the failure to scale up or reuse beneficial local autonomous systems in other organizational units leads to inefficiencies (Kopper & Westner, 2016a). As a result, this leads to wasted resources (Behrens & Sedera, 2004), conflicts with official systems and projects (Klotz et al., 2019), or higher and unexpected financial costs (Zimmermann et al., 2017). For instance, BI reports are developed by various employees, which could have been maintained and reused centrally (Kopper & Westner, 2016a).

2.5 IT risk management

Risk management in the context of SIT details an ongoing process of identifying, evaluating, and controlling the risks (Zimmermann & Rentrop, 2014). As organizations need to understand the potential risk impact and likelihood of events to effectively manage IT related risks (National Institute of Standards and Technology, 2018). This management of risks is crucial for organizations to safeguard their sensitive data, protect critical systems and infrastructure, and ensure the continuity of their operations. As discussed in the previous chapter, the current academic landscape lacks a comprehensive methodology that is specifically designed to handle SIT risks. Consequently, organizations struggle with the complexities of managing SIT without clear guidance or established best practices. Therefore, in this section the established IT risk management frameworks are explored if they can address the unique challenges that are posed by SIT.

2.5.1. IT risk management frameworks

COBIT, ISO/IEC 27000 and NIST are IT frameworks that are internationally recognized as best practice frameworks because they cover in detail the areas of control, governance, risk, and compliance (Goosen & Rudman, 2013; Tøndel et al., 2014). Therefore, the frameworks of COBIT, ISO/IEC and NIST are studied in this section as they address risk management to mitigate the threat of IT security incidents. Studying the IT risk management approach of each framework helps to identify the relevant procedures in managing SIT risks.

COBIT

Control Objectives for Information and related Technology (COBIT) was developed by the Information Systems Audit and Control Association (ISACA), an organization that was founded in 1967 in the United States of America as a response to the growing concerns of computer systems (Taherdoost, 2022). The objective of COBIT is to provide a framework for control to assist an organization with the alignment between the business goals and the use of IT (Haufe et al., 2016). COBIT guarantees this alignment as it enables IT to the business and maximizes its benefits to make sure that IT resources are used responsibly and that IT risks are managed adequately (Gehrmann, 2012).

The COBIT framework helps to guide risk management for identification and management of all IT-related risk was they provide a management objective to support risk management (ISACA, 2018b). APO12 'Managed Risk' is a management objective that is listed in the Align, Plan, and Organize (APO) domain that addresses the overall organization, strategy and supporting activities for IT. The APO12 objective integrates IT related enterprise risk management with overall enterprise risk management and weighs the costs and benefits of managing IT enterprise risk. APO12 states the following six risk management steps to perform: (1) collect data, in this stage the data is identified to support effective IT-related risk analysis, identification and reporting; (2) analyze risk, a verified understanding is provided of actual IT risks to support risk-taking decisions; (3) maintain a risk profile, an inventory is kept of known and related risk, risk resources and risk characteristics, such as predicted frequency, potential impact and responses; (4) articulate risk, inform all necessary stakeholders on the current state in a timely manner of IT related exposures and opportunities for the appropriate response; (5) define a risk management action portfolio, manage possibilities to lower risk to a manageable level as a portfolio; and (6) respond to risk, respond adequately to risk occurrences that materialize and take the necessary actions to reduce the loss (ISACA, 2018a).

ISO/IEC 27000 series

The International Organization for Standardization (ISO) and the International Electro Technical Commission (IEC) publishes the ISO/IEC 27000 series of standards that focuses on security controls and best practices in organization's Information Security Management Systems (ISMS) (Taherdoost, 2022). The ISO/IEC 27001 is a globally recognized standard that addresses the requirements to implement the ISMS and is commonly used together with ISO/IEC 27002 that provides the necessary implementation roadmap for information security controls and recommendations (Bounagui et al., 2019; Taherdoost, 2022). ISO/IEC 27001 is a standard that was mainly designed as an ISMS framework and states only the information security requirements and lacked the proper documentation for information security management (Al-Ahmad & Mohammad, 2012). As a response, ISO/IEC 27005 was published to fill that gap and it provides the methodology in information security risk management (Al-Ahmad & Mohammad, 2012).

The ISO/IEC 27005 standard provides the following seven activities in information security risk management: (1) establishing the context, the necessary criteria, scope and boundaries are set and defined; (2) risk assessment, the identification, analysis and evaluation of risks are developed; (3) developing a risk treatment plan, controls to reduce risks are determined; (4) risk acceptance, the decision of risks are made and properly recorded; (5) risk communication, risk information is shared between shareholders and management; (6) continual monitoring and reviewing risks, to identify changes and provide an activity overview; and (7) maintain and improve the information security risk management process (International Organization for Standardization, 2022).

NIST SP 800 standard series

The National Institute of Standards and Technology (NIST) is a federal agency established by the U.S. Department of Commerce and initially developed the Special Publication (SP) 800 standard series for federal information systems that addresses privacy and security requirements, and it was later adopted by non-federal organizations (Taherdoost, 2022). The NIST SP 800-37 provides the application of a risk management framework in IS and organizations as it sets up a structured approach in controlling IT related risks (Taherdoost, 2022).

A risk management framework is developed in NIST SP 800-37 that addresses security and privacy risks in diverse environments with the following approach: (1) prepare, this includes role distribution, strategy formulation and setting up controls; (2) categorize, organizational risk management processes are informed by terming the adverse impact to assets and operations; (3) select, control baselines are selected, tailored and documented to protect assets and operations; (4) implement, the specified security and privacy controls are implemented; (5) assess, the implemented controls are analyzed that desired outcomes are met; (6) authorize, provides organizational accountability that the security and privacy risk is acceptable; (7) monitor, maintain ongoing situational awareness of the ongoing risk posture (Joint Task Force, 2018).

3. Methodology

In this chapter, the research methodology is discussed, following the design science research framework for IS Research developed by Hevner et al. (2004). Section 3.1 describes the research design where design science research is explained and presented. Section 3.2 discusses the methods of data collection used during the research. Section 3.3 describes the data analysis methods, and lastly, Section 3.4 presents the reliability and validity of the report.

3.1. Design Science Research

As stated earlier in Section 1.4 the design science research consists of two components, a theoretical research component and an empirical research component. Figure 4 describes the overall research structure derived from the IS research framework of Hevner et al. (2004). The environment consists of people, organization, and technology that defines the problem and specifies the business needs, which in this case is to develop an SIT risk management framework. The first step in conducting design science research is to perform an extensive literature review, which is part of the knowledge base within the framework, as this describes the concepts of SIT and risk management. The goal of the literature review is to get a better understanding of the current academic landscape of SIT. The knowledge obtained from the foundations and methodologies in the knowledge base is then utilized in the building phase. Following empirical research, the relevant topics are identified, and the necessary steps to build and evaluate the artifact are taken.

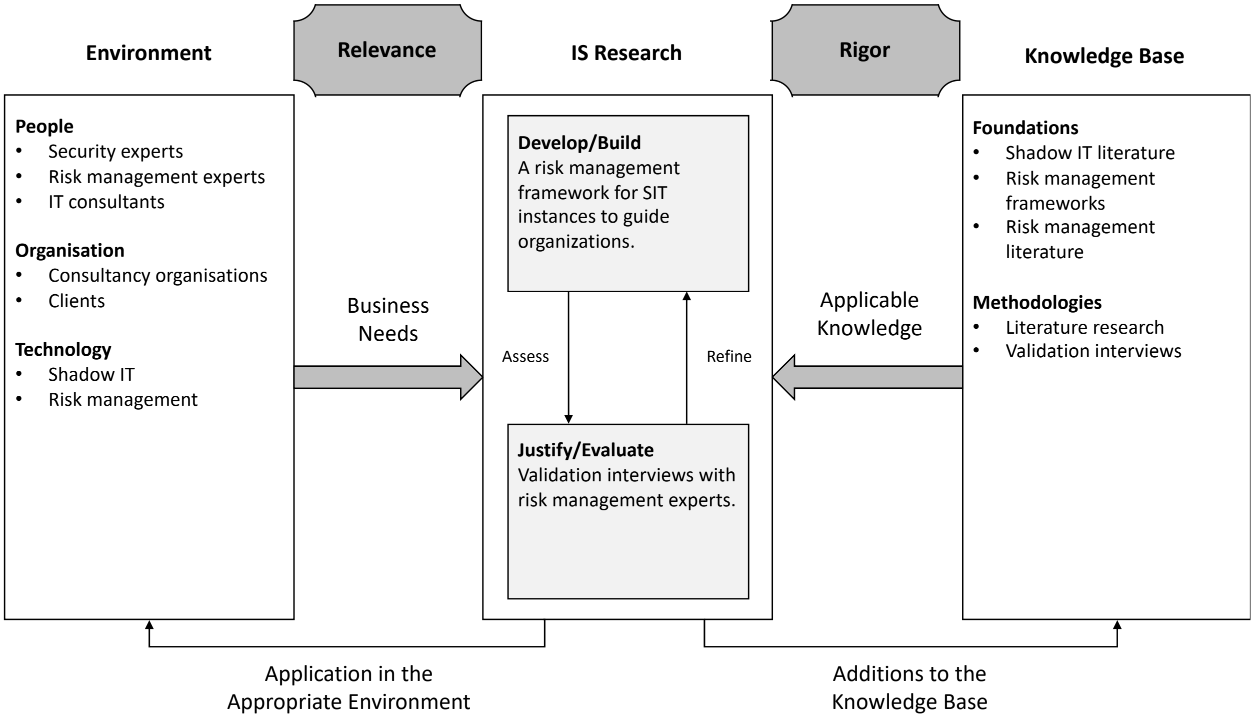


Figure 4. Design science research framework adapted from (Hevner et al., 2004)

The second step of design science research is to perform empirical research, to develop the artifact by conducting semi-structured individual interviews. These interviews will form the conceptualization of the artifact. In this research, the developed artifact is a framework that provides risk management for SIT instances. The conceptualized framework will be then validated by semi-structured individual interviews with experts that were previously interviewed. The results of the validation interviews will lead to the necessary refinements toward the final framework.

3.2. Interview process

The topics that were identified during the literature research helped to understand the key constructs, and knowledge gaps, and build the knowledge for developing the framework. Furthermore, it also develops the interview questions to justify and evaluate the findings. Individual interviews are held with security and risk management experts that are knowledgeable of SIT to build the conceptual framework. The aim of the individual interviews is to gather empirical data that, together with the literature review, address the business needs of the artifact.

3.2.1. Interview approach

To perform a qualitative interview, a romantic interview approach is held to generate rich data. The romantic view explores the participant's subjective experiences, feelings, beliefs, attitudes, and behaviors and tends to reveal a richer and more realistic picture of the design artifact (Schultze & Avital, 2011). The romantic interview approach recognizes the importance of understanding the design artifact in its real-world context. By exploring the participant's beliefs, attitudes, and behaviors, the approach contextualizes the design artifact within the broader social, cultural, and organizational aspects of its use. This contextualization contributes to a more realistic picture of the design artifact's performance and helps identify potential challenges, opportunities, and improvement areas.

A key responsibility of the interviewer within this approach is to encourage and provoke the interviewee's analytical and interpretive skills to generate the desired results. The romantic perspective of interviewing has the following three characteristics (Schultze & Avital, 2011): (1) Grounding the interview in participants' own experiences; (2) Acknowledging and valuing participants' narrative reconstruction of their experiences; (3) Providing an explicit framework for guiding the participants to articulate and interpret their experiences. Therefore, the interview will consist of semi-structured questions, as the open nature of these questions will allow respondents more freedom in their answers in contrast to a simple yes-or-no question. In addition, a laddering interview technique is utilized to explore deeper understanding of the underlying motivations and values of the participant's personal constructs (Schultze & Avital, 2011). This is achieved by asking follow-up questions on how and why participants adopt their perspective on the phenomenon. The advantages of the above interview approach are that the researcher builds trust and rapport, gains deeper insights, and facilitates more productive and focused discussions.

The principles of the general-to-specific rule is followed in conducting the individual interview (Stewart & Shamdasani, 2014). It means that questions are ordered from generic to specific, meaning that more general questions are placed at the beginning, and the most specific questions are placed near the end of the interview. In the application of design science, a semi-structured interview guide is created that follows that rule. By initially asking general questions, the interviewer avoids priming the participant with specific information or biases and allows participants to ease into the conversation. It promotes a more unbiased and authentic representation of the participant's viewpoint The artifact is developed by structuring the interview questions in a meaningful sequence, and ultimately leading to the utilization and evaluation of the artifact (Hevner & Chatterjee, 2010). The final interview protocol can be seen in Appendix B and is estimated to last between 30 to 60 minutes consisting of 11 semi-structured questions.

3.2.2. Sample design

The following approach to sample participants for qualitative interviews is followed (Robinson, 2014): (1) Defining a sample universe; (2) Determining a sample size; (3) Selecting a sample strategy; (4) Conducting sample sourcing. Firstly, the sample universe is established by listing the inclusion and exclusion criteria for the participants that should be met to qualify for the research. The inclusion criteria for this research are that participants should have professional knowledge of SIT and risk management. Participants that lack risk management knowledge, even if they do have knowledge of SIT, are excluded. This is because the research aims to design an SIT risk management framework, which requires risk management knowledge. Secondly, the sample size is determined for the individual interviews. In this research, the number of participants for the interviews are aimed at eight to ten participants due to the chance of data saturation.

Lastly, the sample strategy and sample sourcing are defined. Purposive sampling is used to gather the necessary participants for the research. Purposive sampling is a non-probability sampling method for locating individuals that meet the required criteria in the sample universe and are most likely to provide the desired information (Robinson, 2014). In terms of sample sourcing, the final composition of participants in terms of SIT expertise is considered, as it influences the structure and desirability of producing rich data (Stewart & Shamdasani, 2014). The interview participants are selected together with the company supervisor as this makes identifying suitable candidates easier due to the supervisor's professional knowledge and company network. The organization is a global accounting firm that provides assurance, tax, consulting, and advisory services to its clients, with over 300,000 employees in over 700 offices. To establish a diverse and dynamic environment the experts will vary in specialization and experience as this introduces a more heterogeneous sample and it can lead to more generalizable findings (Robinson, 2014).

Table 3 shows the details of the participants in the individual interviews. Each interview takes place online via the application Microsoft Teams. Microsoft Teams is a workspace and videoconferencing tool that is used as the standard in terms of reliability and security within the organization.

Table 3. Individual interview participants details

#	Specialization	Job title	Abbreviation	Years of experience
1	Risk management, finance, cybersecurity, and service delivery	Partner	P1	33 years
2	Risk management and cybersecurity	Senior manager	SM1	9 years
3	Risk management, cybersecurity, and network infrastructure	Manager	M1	13 years
4	Risk management, cybersecurity, and healthcare	Manager	M2	9 years

5	Risk management, cybersecurity, and finance	Senior	SE1	3 years
6	Risk management, cybersecurity, and finance	Senior	SE2	5 years
7	Risk management and cybersecurity	Senior	SE3	5 years
8	Risk management and cybersecurity	Staff	S1	1 year
9	Risk management, cybersecurity, and data privacy	Staff	S2	3 years

3.2.3. Validation interviews

After the individual interviews have been conducted and the framework conceptualized, it was validated by expert opinions, which makes sure that it has the capability to deal with the problem context. This process is facilitated by conducting validation interviews, participants include previous participants that have the most experience in SIT risk management. The participants are asked validation questions of the designed artifact and its effect, trade-off, sensitivity, and requirement satisfaction questions (Wieringa, 2014). The combination of the above-mentioned questions tests the generalizability of the artifact, its effects, and its satisfactory usage to the problem context. The validation questions that are asked in both rounds can be seen in Appendix D.

The validation interviews are held in two rounds, as the framework will be validated twice. The first round includes all the participants as shown in Table 4, and the artifact will be adjusted accordingly. The adjusted framework will then be validated in a final interview round by participant P1 and participant M1. The feedback given by the experts is utilized to produce a completion of the artifact, as the aim of the validation research is to understand the effectiveness of the artifact in its intended problem scenario.

Table 4. Validation interview participants details

#	Specialization	Job title	Abbreviation	Years of experience
1	Risk management, finance, cybersecurity, and service delivery	Partner	P1	33 years
2	Risk management, cybersecurity, and network infrastructure	Manager	M1	13 years
3	Risk management, cybersecurity, and healthcare	Manager	M2	9 years
4	Risk management and cybersecurity	Senior	SE2	5 years

3.3. Data analysis

Qualitative data analysis is performed during the research to reduce the data to meaningful information, this includes different coding techniques of the transcribed text. Coding is used to identify and assign labels as units to organize the different concepts, ideas, or themes. The most common techniques in coding are open, axial, and selective coding (Recker, 2021): (1) Open coding is a method that focuses on revealing and labeling ideas found in data. These ideas can be classified into broader categories to decrease the number of revealed concepts at a higher level of abstract thinking; (2) Axial coding is a technique that involves arranging groups of concepts with each other and identifies a causal relationship as this helps to differentiate between conditions, action and interactions; (3) Selective coding can be utilized to pinpoint the data to a central category, and then logically link all other categories to that central point. The data is hereby selectively chosen and examined to validate or enhance categories or relationships.

The different coding techniques mentioned earlier produce a filtered, categorized, and rigorous set of codes and themes. After completion of this process the data can be further discussed and helps the design science process in developing the framework.

3.4. Reliability and validity

Yardley (2000) established several criteria for assessing qualitative research, which have become widely recognized as a means of evaluating the validity of a study (Robinson, 2014). Well-conducted qualitative research aims to satisfy the above-mentioned criteria, and these include: ‘sensitivity to context’, ‘commitment and rigor’, ‘transparency and coherence’, and ‘impact and importance’. In terms of ‘sensitivity to context’, the contextual richness is given to find new insights in the risk management of SIT, as existing risk management frameworks are analyzed to identify possible gaps combined with the sampling consideration of the participants from expert interviews that provided their perspective in establishing the artifact. In addition, the focus group has contextual richness as it contains complex arguments between participants in the discussion and needs to be processed appropriately by the researcher.

With regards to ‘commitment and rigor’ and ‘transparency and coherence’, the design science research conducted is committed to producing a complete design artifact and immersing oneself in the relevant research data. The different research methods used during the research are outlined with as much transparency and completeness. The literature review, data collection, data analysis, and research findings are provided with a thick description and presented in a clear and coherent manner. This allows other researchers to understand and replicate this research. The steps to minimize bias and increase validity include triangulation, member checking, and peer review. The findings of the research are shared with the participants to ensure that their experiences and experiences are accurately reflected. In addition, the individuals within the organization of where the research has been conducted peer-reviewed the research and provided the necessary feedback during the research process.

Through qualitative analysis, this study aims to give answers on the discussed phenomenon as the current body of academic literature and organizational practices is limited. Ultimately the research aims to provide academical and managerial relevance, and this contributes to the ‘impact and importance’ of the research. The data that is collected and analyzed aims to present a novel and challenging perspective that opens a new path of understanding the topic.

4. Findings

This chapter discusses the research and findings. The data collected during the interviews is processed through thematic analysis and is shown in Appendix C. The discovered themes and codes from the data analysis are explained and discussed below to support the conceptualization of the framework.

4.1. Determinants of SIT

The determinants of SIT can be divided into enablers, motivators, and missing barriers. This section analyzes the interview results of determinants of SIT.

4.1.1. Enablers

Technical accessibility
In total, half of the participants shared the same reasoning that these tools are readily available and provided by external parties that address productivity needs. As participant SE3 elaborated with the following: *"… most often employees seek out alternatives that are readily available".* Participant SM1, for instance, mentions that users find it sometimes more convenient to share client files with their personal OneDrive or Dropbox application because of accessibility and convenience. Similarly, participant S1 states that Google Translate is a popular tool because of the ease of use, availability, and performance but that their organization clearly states that they need to use their own provisioned translation tool due to privacy concerns. Participant SE1 also mentioned that currently ChatGPT is a popular external office productivity cloud application but that users need to be observant not to share any confidential data.

IT user competence
Participants noted that employees are becoming more tech-savvy and are working independently without the involvement of others to find more productive solutions in their work. Participant SE2, for instance, states the following: *"I think that employees are getting smarter in conducting their way of working to save time and hassle whether it is with tools provided by their company or external tools".* Participant M1 further comments that employees always want to find the most efficient way of doing their work.

4.1.2. Motivators

Poor business-IT alignment
A lack of alignment between BUs and IT departments can enable the prevalence of SIT, half of the participants have noted this as a possible determinant. Participant SM1 mentions that the shift in responsibility has caused a divide between responsibilities as he states the following:

> *"Throughout the years, the responsibility has increasingly shifted towards the business because they are the end-users of the cloud service. In addition, the IT department is not even involved in the actual purchase or use of these services. I would say that IT departments would not be responsible for SIT management."*

Following from the above statement, participant M2 mentions that managed applications and tools are more central from a business point of view. Participant S2 also agrees that the business is more responsible for managing the IT assets. Due to this contrast in determining a proper alignment between

BUs and IT departments, participant P1 argues that it makes it difficult for IT departments to receive and determine the proper budget for a well architected security network. Participant S1 further elaborates that when there is a divide between the two departments it becomes more difficult to get a clear and accurate view of the organization's overall assets.

Shortcoming of IT systems

Roughly half of interviewed participants outline that the main cause of SIT usage is that employees are facing issues with the existing company provided tools and therefore look for alternatives. Participant SE2 shared his opinion with the following: *"When a company provides tools that are very difficult to use then it is more likely for an employee to consider the use of SIT".* Participant P1 shares that individuals also just want to perform their work duties but when they face hindrance with the existing provided tools, then they will look for alternatives. One of the reasons that participant M1 mentions is that employees look for alternative tools that save them time and to work more efficiently.

4.1.3. Missing barriers

Misalignment of IT governance

How IT is governed within organizations regarding policy and guideline-making can be a determinant of SIT adoption. During the interviews, many of the participants mentioned several reasons why there is a misalignment of IT governance within organizations. Participant SE2 provides the following statement: *"Organizations do have security measures in place, but a lot of organizations do not put much consideration into SIT risks. The organizations don't consider SIT as a high risk".* This is strengthened by participant SM1 saying that *"Some other organizations don't mind SIT that much or are not aware of it".* Participant SE2 also outlines that companies do not know how to manage SIT appropriately. A possible reason why companies cannot manage the risks of SIT is provided by participant S2 who states the following:

> *"The pitfall for organizations is that they have a lot of cybersecurity measures, but don't have an idea of their total asset management. Then it becomes really hard whether those controls are justified."*

However, participant P1 has noted that "… not all companies are scanning the whole internal network and if you scan the network then you mostly do it for detecting unpatched systems and systems that can have vulnerabilities because of misconfigurations". Therefore, even when organizations scan their overall network, they are primarily doing it for vulnerability issues and not SIT risks. He continues by saying that many companies do not spend the resources and time to monitor suspicious network traffic, and this is even more difficult for unauthorized devices. Participant M2 states that organizations do have security controls implemented for security incidents but in a lot of cases do not look if it has been caused by SIT. This can indicate that SIT is not a priority for the organization. Furthermore, participant P1 comments that some organizations mention the use of SIT in their end-user policy either implicitly or explicitly, which makes it quite unclear whether the user's actions are compliant. Participant M1 mentions that he rarely heard that employees are fined but more often reprimanded for using non-approved external tools. He also outlines that organizations should take into consideration the geo-political factors in using cloud solutions because some cloud solutions are banned in other countries.

Lack of awareness

Half of the participants have noted that employees are not aware of the associated risks or of existing IT policies. As participant M1 states the following: *"It's more a lack of user awareness that they are creating a specific risk for the organization".* Participant M2 also says that most individuals don't call the SIT instances SIT and if the tool works accordingly then everybody will believe that is part of the IT landscape within the organization. Participant SE2 comments the following: *"Another reason is that employees are unaware that they are not compliant with organizational policies".* Participant P1 states that this occurs because users don't always feel that they are using a third-party tool for their business needs. He further outlines that employees within a large organization don't know who to address when they face certain issues.

4.2. Effects of SIT

Based on the interview results, most participants indicated that SIT has more negative effects than positive effects. A few participants briefly mention the positive effects of SIT. This section analyzes the results of positive effects and negative effects.

4.2.1. Positive effects

Interacting with SIT can improve organization productivity, technological innovation capabilities and user satisfaction. Participant SM1 argues that the user needs to have a certain freedom for productivity and innovation. Moreover, he mentions that SIT is convenient for individuals which resulting in enhanced user satisfaction by giving the following example:

> *"For example, when I first started within the organization, I had to make a lot of screenshots and edits of documents. I got the recommendation from a colleague to use an alternative open-source software application. But strictly speaking, that's also considered as SIT, because it is not authorized by the organization. Usually, SIT is the result of the laziness of the user. It is not necessarily always bad."*

Furthermore, he continues his reasoning by saying: *"I do not think SIT as a whole should always be fully avoided. If you are allowed to only use authorized software by the organization, there are a lot of exceptions where this may slow down innovation or productivity as a whole"*. However, he thinks the major risks related to SIT should be reduced as much as possible. Participant S1 agrees with this and indicates that individuals do not consider the information risks for the organizations and only see the productivity of the tool.

4.2.2. Negative effects

Security risks

When asked about the effects of SIT, security risks were also frequently mentioned by the participants. Participant SE3 indicates that the main risk of using SIT is weakening network security in the organization. Furthermore, participant P1 and participant S1 explain that the organization is very dependent on how employees handle the information. Participant S1 continues by saying that data confidentiality is at risk because data can quite easily get outside the organization through SIT. Moreover, participant SE2 agrees with this and clarifies that statement with the following example:

> *"The most common risk is the use of third-party file transfer tools, which may not be managed by the BU and thus companies do not know where that data is being processed and whether it is secure."*

Moreover, half of the participants mention if employees are not compliant with the company policy that it could lead to a data breach. Participant SE1 outlined this further with the following statement: *"If you're working with confidential data that is cybersecurity related or incident related and to use applications outside of the company can be considered a risk"*. Participant S2 indicates the following example: *"The individual risk is that a person's data due to SIT usage is published without consent or that an entity uploads personal data into the cloud without permission. That would be a data leak where individuals or an organization processes data without consent"*. Therefore, he believes that compliance with privacy laws and regulations must be considered.

Integration risks & data inconsistency

Low degree of integration can lead to data inconsistency. Four participants note that the use of SIT can harm the confidentiality, availability of services and the integrity of data. Participant M2 further clarified by giving the following statement: *"... the data being entered in the SIT application cannot guarantee that it is also implemented in the central IT application appropriately"*. He continues by saying if information is put in in a separate system that differs from the main IT applications, then during the auditing process incorrect statements may surface. He also gives the following example:

> *"I have had multiple situations where I have heard that certain departments would use a specific SaaS solution to plan something that went outside of the normal planning application. You would always hear that it would lead to data issues such as inaccuracies or that it did not contain the appropriate information."*

Participant M1 mentions that most of the time that they are not aware when employees are using a separate system where they are using specific tools, for instance for purchase orders. Furthermore, participant SE3 indicates that it is a challenge to address the employees to quit using SIT application, when the whole team has set up a whole work process that runs on SIT.

Control loss

A pattern that can be seen in the interviewees' answers is that many of the participants mention control loss as a negative effect of SIT. The most common reason of control loss is because there is limited to no security controls within organizations since existing SIT instances are unknown. Participant SM1 believes that it is problematic for organizations if you do not know which IT assets you are managing, resulting in SIT users. Participant SE2 agrees with this and states the following:

> "*Organization cannot meet security controls when individuals manage corporate data on SIT instances. As you cannot manage the security settings such as password settings in contrast to company managed tools."*

He indicates that this causes limited abilities for an organization to take the necessary protective measures, and also lacks a complete oversight of its IT landscape. In addition, participant SE1 mentions that if organizations make use of cloud solutions, they do not know where the information is stored and for how long it will be stored at the cloud vendor. Moreover, he indicates that it is important to have security controls, since the organization is working with the confidentiality of clients. He provides the following statement: *"You have certain agreements with clients that you only use approved tools and to ensure that data is being kept securely and appropriately"*.

Synergy loss & inefficiency

Not optimally scaling up or reusing useful local autonomous systems in other organizational units leads to loss of potential synergies and inefficiencies. According to participant M2, since there are different systems for one business process, you never know which data source is the most correct one. Furthermore, he and another participant mentioned that it influences the financial costs of the organization. However, participant M2 states that SIT is not always bad, it becomes an issue when groups of people start using it, leading to inefficiency. Participant P1 outlines the following example:

> *"An example is that an organization uses a freeware service that acts as a collaboration tool, but within a short time a large proportion of employees begin using it. Then the organization must decide whether to remove or approve and purchase the software including considering it for additional security features within their work environment."*

Participant S2 believes that the most organizations do not have a complete insight into all their IT assets. He gives the following statement: *"In terms of software and hardware, they are unaware of what information runs through their organization"*. Participant SE2 agrees and add to this by saying: *"… organizations struggle to identify the entire SIT landscape"*. Participant M1 states the following: "*We have a system for keeping track of certain processes, but we do not know if other BUs use another system for creating purchase orders"*.

4.3. IT risk management

In this section the field of IT risk management is explored, and insights are given to the current landscape and actions that an organization can perform to mitigate SIT risks.

4.3.1. Current landscape

All participants state that they are not aware of any specific SIT framework that can manage the associated risks. Participant M1 outlines the following statement regarding the current landscape of SIT management:

> *"I'm not aware of any specific frameworks that are designed for SIT that are available. I think it's embedded within the current available risk frameworks because it's quite a specialist topic, but it's more regarding software asset management. However, I think that the current embedded frameworks could be better in addressing SIT."*

Participant S2, participant SE3, and participant SM1 do mention that the NIST framework briefly explains the risks of SIT. However, SE1 argues that it does not have the specific details that can address the risks of SIT. Participant P1 mentions the following: *"Most of the popular security frameworks don't follow NIST but follows Center for Internet Security (CIS) controls and it aligns with the list of SANS top 20".* He further comments his belief in the existing risk management landscape by sharing the following remarks:

> *“An organization becomes efficient when they need to move from implementing what they don’t want to have towards enforcing to what they allow. Currently we adopt a stance that everything is allowed unless certain criteria tell otherwise, but we need to move towards an approach that nothing is secure. That is practically the way forward and that is also part of the Zero Trust architecture.”*

Moreover, participant SE2 is working with a governmental organization that implements the Baseline Informatiebeveiliging Overheid (BIO) to implement cybersecurity measures and is based on the ISO 27000 series that addresses SIT risks. However, he also mentions the following: “*I believe that the BIO that follows ISO 27001 only states that when SIT is active within the organization that you have to identify it and fix it. It only states that and it does not go deeper than that and merely acts as a guideline and does not provide enough guidance to the full scope”.*

4.3.2. Prevent

All participants mention preventative actions and this ranges from creating a policy regarding the usage of SIT, implementing filter controls on software and hardware, and creating awareness and facilitating training on SIT.

Create a policy on SIT usage
Participant M1 states that the organization first needs to determine the risks of SIT and then create a policy of which kinds of software and hardware are excluded from the environment. He continues with saying the following: “It also depends on the individual and job title in who needs to use the SIT environment”. In addition, participant P1 states that an organization should adopt a policy that states which IT tools are allowed otherwise an organization cannot identify the unauthorized tools. Participant M2 argues that agreements between suppliers are needed to determine who exactly is liable when a data leak occurs. He further comments that policy making is dependent on managing individual responsibility and determining the amount of trust to give to employees which is unique for each organization and might differ between departments and BUs. He further mentions that employees can also be reprimanded from using SIT by taking disciplinary action. He comments the following:

> *“If policies are breached then you can fire them or you can act against them, which in turn also prevents people from doing it because they know they will be held liable.”*

In addition, participant S2 states that organizations are obliged to comply with laws and regulations and that repercussions can be given to individuals or organizations in the form of penalties. Moreover, he argues the following for organizations: *“To ensure that SIT is part of the code of conduct and that employees know which behavior can lead to specific sanctions”.*

Awareness and training
When asked about capabilities within a framework, almost all the participants determined that creating awareness is an important topic to address for preventing SIT risks. Participant M1 states the following: *“I think creating awareness for the employees is the biggest challenge for a company”.* Participant P1 comments that users need to be very aware to not use SIT tools. Participant S2 says the following regarding awareness:

> *“They have to comply with the organization’s code of conduct and penalties are included. An employee should be aware of the risks they are facing when they process sensitive information with external tools. Because it is their own responsibility when they upload the information.”*

However, participant SM1 says that security awareness is very often not translated to actual secure behavior. It is noted in terms of behavior that four participants agree that employees should file a request to either the IT department or the BU for approval of a SIT tool and otherwise ask for suitable alternatives. Participant SE3 states the following regarding responsibility of IT departments and BUs: *“I think it's a shared responsibility because when you look at security awareness. All BUs and all IT people need to be trained on these security issues. Everyone has a responsibility in terms of each control”.* Four other participants agree that awareness training is an effective tool for organizations to raise awareness and mitigate possible future risks. Participant SE1 state that education is important because simply blocking the SIT instances doesn’t work as people will find a way to circumvent it.

In addition, Participant S2 and participant M1 state that the training can be in the form of workshops, simulations, web learnings or interactive training. Participant SE3 comments the following regarding facilitate training: *“There's a lot of research showing that new forms of training can be implemented to harden the employees and to create a more security aware organization. The training sessions can be simulation exercises in which different scenarios are played out and employees need to respond to that and will learn from it. Those simulations are more ingrained in employees’ memories than conventional training methods”.*

Information security

In terms of having preventative controls in the software and hardware within organizations, as participant SE2 notes it as an important aspect in containing SIT that are deemed as high risk. Participant S2 mentions the actions: “Organizations can take preventive measures, such as policies in which they restrict certain services or devices with logging, monitoring, whitelisting, blacklisting, firewalls, and VPN’s”. Moreover, participant M1 says that organizations can maintain a whitelist for allowed tools and a blacklist for blocked instances. Participant SM1 and participant P1 both argue that external software providers can manage authorized devices and applications in terms of filtering, blocking, and assigning user access rights to a device or piece of software which determines which IT assets a user can utilize. In addition, participant M2 argues that the organization can adopt the following measure for employees:

> *“You have to provide a reason why you're installing it. I can guarantee you that IT in the background is running a scan on our laptops and if they find any software that is not in the list of approved software for which the license is needed, you will get an e-mail and you will get a call.”*

Participant P1 states that cloud services can be filtered by setting up a firewall that can block certain URL’s from being visited. However, he further states the following: “At the moment most filtering is based on unwanted network traffic. If you are going to filter on what is allowed instead of what is not allowed, it means that you can issue a better filter in company data traffic”. He further comments that authentication controls can be set up for physical hardware as a preventative measure.

4.3.3. Identify

All the participants stated that identification should be the first action an organization should take to manage their risk landscape. Participant P1 states the following reasoning: *“The first rule to follow is to know your hardware and the second one is to know your software. If you don't know both assets, then you can’t protect what you don’t know. Implicitly, protection against SIT is to follow rule number one and two …”*. Participant M1 further comments that asset management is therefore important for an organization. Participant S2 also shares that reasoning as he states the following: *“I recommend controlling the organizational information flows. Because it is very hard for an organization to determine the right cybersecurity or privacy measures when they have no control of their information flows.”.* He also continues by saying that the priority to identify all the information flows is lacking in a lot of information security policies and frameworks.

In addition, several participants mention setting up a configuration management database (CMDB), which keeps track of all the organization’s information assets. Participant SM1 outlines the following advantage of implementing a CMDB:

> *“... identification of SIT would be to use software tooling to scan all the assets on the network and compare that to the CMDB that is in place. Any difference in terms of unaware assets within your IT landscape are shown and detected.”*

Participant S2 mentions that an organization can make use of asset discovery and monitoring tools to identify all the hardware and software in an organization and states that Microsoft Defender can be used for that purpose.

Ticket management
A ticketing process was highlighted by three participants as a ticket is created for the organization to get notified and keep track of the status. Participant SE3 elaborates this process as follows: *“Ideally you would have somebody reporting the SIT instance or that it came from network monitoring tools. A ticket should be created of the security incident so that it can be tracked until the risk has been resolved”.* It is good to consider organizations to maintain a safe workplace and that people can anonymously report the issue. In addition, both participant P1 and participant S2 mention that when an employee should have a question, that they can submit a request to the IT department for better services or for the allowed use of a SIT tool.

4.3.4. Evaluate

Six participants have mentioned that after the identification process, the identified instances should be evaluated. As participant M2 states: *“You need to have risk evaluation. To determine accepted risk and the degree of trust in people that would normally be a kind of risk evaluation control to take”*. Participant SM1 also mentions that during the risk evaluation it is important to determine which specific assets are under the organization’s control and which are not. Participant SE2 comments that the impact of SIT on the overall organizational risks should be determined to estimate the SIT risk appetite. In addition, three participants mentioned that the SIT instances should also be evaluated if it is compliant with organizational and regulatory policies in terms of privacy and security. As Participant M1 states the following: *“Organizations should determine their own security policy to determine which controls are* *needed to secure their environment for employees to comply. If SIT applications are compliant with the GDPR but clashes with the company policy, then it should not be used"*.

SIT type and risk impact

Participant SE2 states that organizations should address ways to identify and manage the different types of SIT. As discussed in the literature review earlier, there are four different SIT types which includes, unauthorized cloud services, self-made solutions, self-installed applications, and self-acquired devices. Both participant SE2 and SE3 comment that each of the four needs to have different measures in place and require different types of management, as all four instances can be seen as a severe risk for organizations. Although, SE3 states that installed applications do require the most security controls to ensure a secure work environment.

Two participants state that self-installed applications pose the most risk for an organization as participant P1 comments the following: *"I think installing software can be considered as the highest risk. The risk doesn't only imply that you can leak data to the external environment, but it can also be used by third parties to break into your network".* Participant P1 further outlines that the highest risk is considered when malicious software enters the premises of the internal network and would not differentiate between the other types as it depends on the management of each instance. In addition, participant S2 argues that installed applications may introduce vulnerabilities in the organizational network.

In terms of unauthorized cloud services, four participants comment that it poses a severe risk for an organization. They mention that a loss of ownership in data is an important issue in terms of privacy and control. Participant S2 states the following reasoning:

> *"I would consider cloud services as one of the biggest risks. Because it's a control problem in terms of data privacy, because it is hard to determine who is the owner of the data and who should take the necessary measures. When the data resides in the cloud it is no longer within one organization's control regarding what is happening to the data. The organization must trust the cloud service provider that they do not share the data with other third parties."*

Moreover, two participants mention that the use of self-acquired devices poses a major risk. The reason behind this is because of loss of control and data security. Participant M1 provides the following statement: *"I believe that the use of personal devices can be deemed as one of the highest risks, because the IT department determines by default which applications are installed on company devices. The use of organizational data on a personal device is a total black box. If they're using the laptop at home, where they can use file transfer applications such as Google Drive, Dropbox, etc. then it is not routed to the company network. Because also when working from home you are not connected to the organizational network where a company could block specific websites".*

Participant M2 mentions that self-made solutions can pose a risk and that is regarding developing Excel macro's which through faulty coding can result in loss of data or even worse incorrect data. He also states that there is a risk that if more people become dependent on it and no maintenance of the software is upheld to keep it running then it becomes a bigger problem.

4.3.5. Analyze

It is stated by seven participants that conducting analyzing activities are necessary for an organization to conduct whether to determine whether a SIT instance is appropriate or to identify other alternative tools. Participant P1 states the following: *"A company first needs to determine the existing friction within the IT landscape and determine the reason why people use SIT".* Participant SE2 elaborates the reasoning why people use SIT by providing the following statement: *"The core collaboration between the company and the employee is that the company needs to provide good enough, easy to use and secure tools for employees to perform their work".* Participant SE1 also argues that the organization should not immediately block each SIT instance because that makes it difficult for individuals, but to also identify and address their own shortcomings in their IT and otherwise look for suitable alternatives. Participant SM1 shares the following opinion on the topic:

> *"*There's a bit of a tradeoff made between the essential high-risk applications an organization wants to reduce and the lesser SIT risks that are acceptable. I think that the challenge is striking a balance in determining the risks and to what extent do you allow it."

Participant M1 follows up with the above statement that when an SIT instance operates in a gray area that further investigation needs to take place and says the following statement: *"They should also look at the number of users and for which purposes the SIT tool is used".* During the analysis, participant SE3 comments that an organization needs to analyze the usage patterns and activity levels of the SIT instances to get a clear judgment whether to approve or deny it. Participant P1 argues that an organization needs to improve their existing tools to address the overall issue when they determine to block a SIT instance.

4.3.6. Respond

A respond phase is considered deemed important by six participants. Participant SE2 says the following: "The next steps should be that you take a risk-based approach and determine which SIT is problematic and per SIT instance determine to accept or block it". He continues that an organization should address and prioritize the most severe risks and to follow up from that. Participant SE3 comments that the decision is based on whether it strengthens the organization's overall network security. He continues with the following statement: *"The best approach to managing a security incident is to have a procedure in place. This includes detection and response and that is always based on the organization's procedures".* Participant SM1 and participant S2 both argue that vulnerability scanning is also needed to maintain a correct asset inventory and to prevent vulnerabilities in the network to proceed with the best action.

4.3.7. Monitor

Six participants have stated that monitoring activities are needed to detect irregular activities. As participant P1 mentions the following: *"Organizations need to have continuous security controls to monitor and manage their assets".* He further elaborates that a possible option is to proactively monitor and block internet traffic in advance. That is to enforce a firewall that sets alerts or automatically blocks unwanted instances and to approve only authenticated devices and software within the company network. Participant M1 argues that when the SIT instance is approved that it should be monitored continuously based on the determined risk factors. Participant SE3 says that the monitoring activities can detect and act ahead of time before it turns into a serious problem. However, he continues by saying the following: *“The main challenge is the detection capability because automated monitoring and manual monitoring of such instances is hard to implement”.*

5. Framework

This chapter discusses the artifact design in the form of a framework that is developed based on literature research and empirical research. The framework will provide a risk management guideline to mitigate SIT risks for organizations. Section 5.1 will describe the artifact design process that led to the overall framework. Section 5.2. provides a detailed description of the risk management framework. Lastly, Section 5.3. outlines the validation of the designed framework to test the overall quality and usefulness.

5.1. Design process

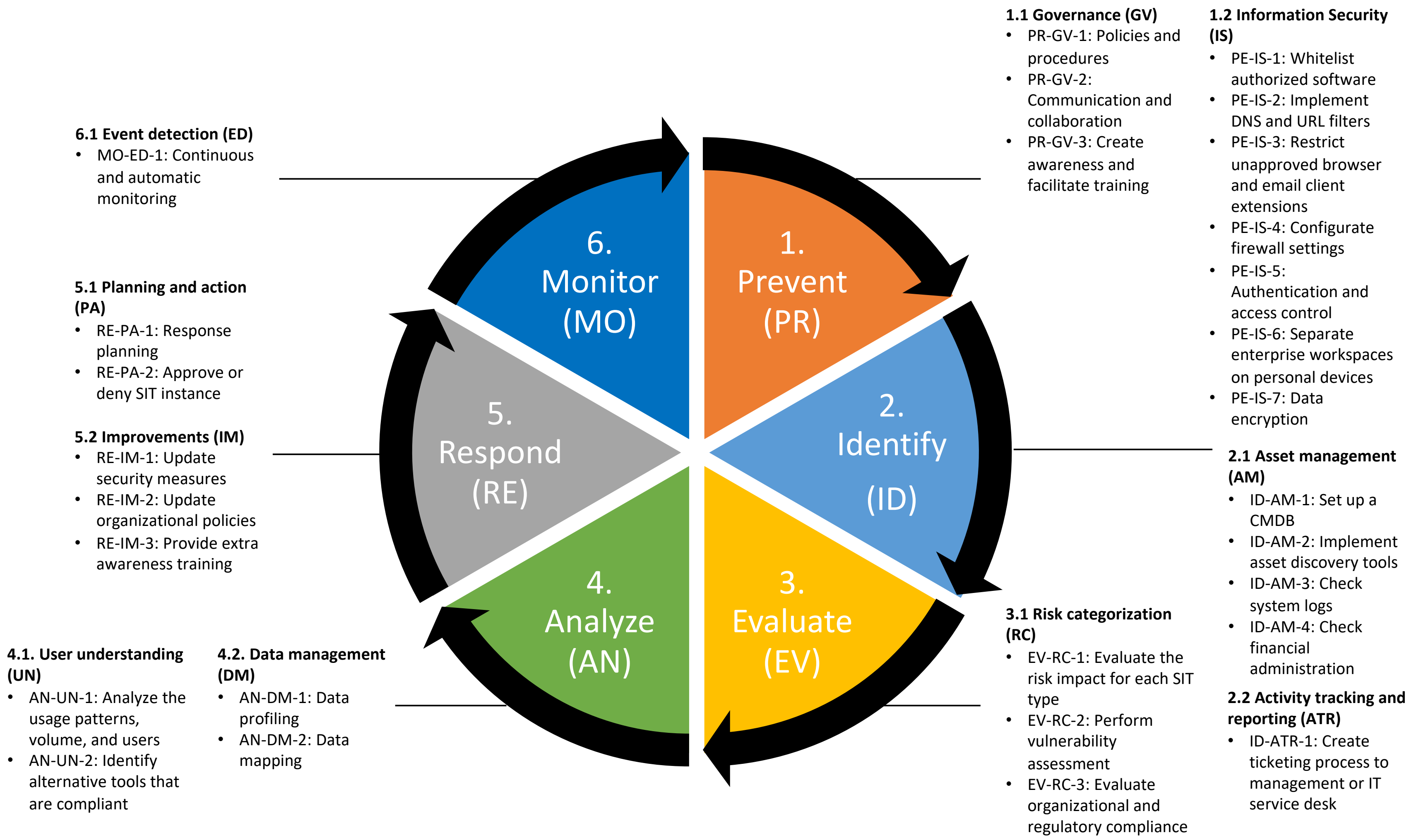
The literature research and empirical research helped to understand the different risks, determinants, effects, and mitigation methods to address the risks of SIT. The developed framework is partially based on existing IT risk management frameworks COBIT, ISO/IEC, and NIST. It has been discussed in the literature research and empirical research that they do not cover the whole landscape of mitigating SIT risks. In this research triangulation is used to combine the multiple frameworks with the empirical research into a more comprehensive and effective framework that incorporates the best practices and controls from each framework and addresses the unique challenges and characteristics of SIT (Recker, 2021). This approach provides a robust and effective solution to the challenges of managing SIT and enhances the reliability and validity of the findings. The developed SIT framework lists mitigations that an organization can take that are sorted in six phases to reduce SIT risks. Table 5 shows how the developed framework is derived from the other frameworks. The next section will discuss the framework and the six phases in detail to address and manage the risks and determinants of SIT.

Table 5. SIT framework development

COBIT APO12 **(**ISACA, 2018)	**ISO/IEC 27005** **(**ISO, 2022)	**NIST SP 800-37** (Joint Task Force, 2018)	**SIT framework**
Collect data	Establishing the context	Prepare	**Prevent**
	Risk assessment	Categorize	**Identify**
Analyze Risk	Risk treatment plan	Select	**Evaluate**
Maintain a risk profile			**Analyze**
Articulate risk	Risk acceptance	Implement	**Respond**
Define risk management action portfolio		Assess	
Respond to risk	Risk communication	Authorize	
-	Continual monitoring and reviewing risks	Monitor	**Monitor**

5.2. Framework description

Participants mentioned integrating cybersecurity controls from the CIS control framework and the NIST cybersecurity framework for the development of the SIT framework. The conceptual framework is partly inspired by those frameworks to effectively mitigate the risks of SIT and adopts an iterative approach. The framework consists of six phases and its corresponding tasks to mitigate the risks of SIT. Figure 5 outlines the conceptual framework, and the next sub-sections elaborate each risk management phase of the framework.



1.1 Governance (GV)

- PR-GV-1: Policies and procedures
- PR-GV-2: Communication and collaboration
- PR-GV-3: Create awareness and facilitate training

1.2 Information Security (IS)

- PE-IS-1: Whitelist authorized software
- PE-IS-2: Implement DNS and URL filters
- PE-IS-3: Restrict unapproved browser and email client extensions
- PE-IS-4: Configurate firewall settings
- PE-IS-5: Authentication and access control
- PE-IS-6: Separate enterprise workspaces on personal devices
- PE-IS-7: Data encryption

2.1 Asset management (AM)

- ID-AM-1: Set up a CMDB
- ID-AM-2: Implement asset discovery tools
- ID-AM-3: Check system logs
- ID-AM-4: Check financial administration

2.2 Activity tracking and reporting (ATR)

- ID-ATR-1: Create ticketing process to management or IT service desk

3.1 Risk categorization (RC)

- EV-RC-1: Evaluate the risk impact for each SIT type
- EV-RC-2: Perform vulnerability assessment
- EV-RC-3: Evaluate organizational and regulatory compliance

4.1. User understanding (UN)

- AN-UN-1: Analyze the usage patterns, volume, and users
- AN-UN-2: Identify alternative tools that are compliant

4.2. Data management (DM)

- AN-DM-1: Data profiling
- AN-DM-2: Data mapping

5.1 Planning and action (PA)

- RE-PA-1: Response planning
- RE-PA-2: Approve or deny SIT instance

5.2 Improvements (IM)

- RE-IM-1: Update security measures
- RE-IM-2: Update organizational policies
- RE-IM-3: Provide extra awareness training

6.1 Event detection (ED)

- MO-ED-1: Continuous and automatic monitoring

Figure 5. Conceptual SIT risk management framework

5.2.1. Prevent (PE)

The “Prevent” phase in the framework aims to prevent the SIT determinants from occurring in the first place. It is important for an organization to understand the necessary criteria to address the possible risks that are caused by SIT determinants. Therefore, organizations must establish the context of their IT environment and prepare accordingly. During the empirical research participants noted that an organization should determine the underlying motivations behind SIT usage and understand its own shortcomings. The prevent phase addresses and prevents SIT determinants that could lead to the potential SIT risks. The categories within the “Prevent” phase include governance, human resource management, and information security. Table 6 outlines all SIT determinants that are drawn from literature research and empirical research, the mitigation tasks address each SIT determinant within the “Prevent” phase.

Table 6. Mitigation tasks for SIT determinants

Technical accessibility	**Mitigation tasks**
• Technical accessibility is increasing as IT complexity decreases and technology offerings expand (§ 2.3.1.). • Employees use readily available alternatives (§ 4.1.1.). • Users share confidential data with personal applications (§ 4.1.1.).	• PE-IS-1: Whitelist authorized software • PE-IS-2: Implement DNS and URL filters • PE-IS-3: Restrict unapproved browser and email client extensions • PE-IS-4: Configurate firewall settings • PE-IS-5: Authentication and access control • PE-IS-6: Separate enterprise workspaces on personal devices • PE-IS-7: Data encryption
IT user competence	**Mitigation tasks**
• IT knowledge availability is increasing in BUs (§ 2.3.1., § 4.1.1.). • Users work more independently (§ 4.1.1.).	• PE-IS-1: Whitelist authorized software • PE-IS-2: Implement DNS and URL filters • PE-IS-3: Restrict unapproved browser and email client extensions • PE-IS-4: Configurate firewall settings • PE-IS-5: Authentication and access control • PE-IS-6: Separate enterprise workspaces on personal devices • PE-IS-7: Data encryption
Poor business-IT alignment	**Mitigation tasks**
• Lack of communication between business and IT departments (§ 2.3.2., § 4.2.2.). • Difficulties budgeting for proper IT resources (§ 4.1.2.). • Difficulties in a proper oversight of all IT assets (§ 4.1.2.).	• PR-GV-1: Policies and procedures • PE-GV-2: Communication and collaboration
Shortcomings of IT systems	**Mitigation tasks**
• Gap between the offered IT systems and the users’ requirements (§ 2.3.2.). • Lack of features in existing systems (§ 2.3.2., § 4.1.2.). • Hindrance of existing company provided tools (§ 4.1.2.).	• PR-GV-2: Communication and collaboration

Misalignment of IT governance	Mitigation tasks
- Missing or too strong technical IT restriction policies and guidelines (§ 2.3.3.). - Implementation of IT restrictions policies have limited effects (§ 2.3.3.). - Employees do not agree with existing guidelines (§ 2.3.3.). - Organizations do not prioritize the dangers of SIT (§ 4.1.3.). - Companies do not invest in monitoring for SIT activities (§ 4.1.3.).	- PR-GV-1: Policies and procedures - PR-GV-2: Communication and collaboration - PR-GV-3: Create awareness and facilitate training
Lack of awareness	**Mitigation tasks**
- Employees are unaware of the existing IT policies (§ 2.3.3.). - employees are unaware of the potential impact of SIT (§ 2.3.3.). - Users are unaware of using a SIT instance (§ 4.1.3.).	- PR-GV-1: Policies and procedures - PR-GV-2: Communication and collaboration - PR-GV-3: Create awareness and facilitate training

Governance (GV)

The governance category is comprised of establishing policies and procedures (PR-GV-1) and ensuring communication and collaboration (PR-GV-2). The governance task PR-GV-1 aims to establish clear policies and procedures around the use of IT assets within the organizational network. This task addresses the alignment of IT governance. During the policy-making process organizations need to understand the degree of trust they should give their employees. The policies should define in which manner and usage IT assets are allowed in terms of installed applications, cloud services, personal devices, and self-made solutions. The policy should be explicitly made clear for employees to avoid user misunderstandings or lack of knowledge. Geo-political factors and its regulations need to be considered for the allowance of IT instances. The organization should consider implementing a BYO policy to address the use of personal devices and address remote work policy and procedures. Furthermore, organizational policies need to comply with laws and regulations. The organization can impose fines or penalties as deterrents for individuals when a certain policy is breached. The policies and procedures that are set up for allowed IT instances leads to a better identification of unauthorized SIT instances.

Moreover, the governance task PR-GV-2 can mitigate the determinants of business-IT alignment and shortcomings of IT systems. The task ensures that effective communication and collaboration is in place between the departments. The departments need to be transparent towards each other and communicate business goals to foster a shared understanding of business objectives and IT capabilities. By promoting open communication and encouraging collaboration, organizations can facilitate a stronger alignment between business and IT, leading to improved decision-making and resource allocation to address SIT security risks. Collaborative efforts enable the co-creation of solutions that ensures that IT systems adequately support business processes and align with organizational goals. The task enables a deeper understanding of user needs and preferences. The communication of departments and BUs can extend towards involvement of individuals in addressing the gap between offered IT systems and users' requirements. This can lead to reducing the need for employees to seek alternative solutions in SIT.

Organizations should invest in staff training and awareness programs to ensure that all employees understand the risks associated with SIT. The task PR-G-3 trains and ensures that employees are equipped to make informed decisions about the use of the different types of SIT instances these include personal devices, installed applications, self-made solutions, and cloud services. This training should include best practices for securing data and systems, as well as educating employees on the potential consequences of non-compliance with organizational policies and procedures. Training can be in the form of workshops, simulations, web learnings, or interactive training. The IT department and BUs have a shared responsibility to facilitate such training and awareness programs. The organization should measure its impact and whether the awareness training is translated to secure behavior and otherwise adjust accordingly.

Information security (IS)

The determinants of technical accessibility and IT user competence can be prevented by implementing protective technology measures to hinder unwanted applications and devices into the organizational network. These measures are divided into tasks in which the organization can manage their IT assets to prevent SIT from occurring. These tasks establish the ground rules in protecting the network from unauthorized SIT instances. The task PE-IS-1 includes setting up a whitelist for cloud services, installed applications, and self-made solutions that only allows authorized software to be executed or accessed. This task makes sure that the right technical controls are in place such as that only specific file types and software vendors are allowed and utilized. Blacklisting controls should also be considered to deny harmful SIT instances from accessing the company network. The task PE-IS-2 addresses DNS and URL filters to prevent users from accessing unapproved and potentially harmful domains and websites. The implementation of filters can include category-based filtering, reputation-based filtering, or using block lists to prevent security risks (Center for Internet Security, 2021). In addition to blacklisting, the task PE-IS-3 aims to restrict unapproved and unauthorized browser or email client extensions that are deemed harmful towards IS security.

An organization should also prevent unwanted devices and unauthorized users into their network that may cause harm. The use of SIT in the form of unidentified personal devices and users should be prevented from accessing the company network. Task PE-IS-4 configuration of firewall settings and task PE-IS-5 that discusses authentication and access control can address that issue. PE-IS-4 should configure firewall settings that isolate unauthorized traffic from end-user devices to reach critical company servers. The implementation methods include setting up a virtual firewall, operating system firewall, third-party firewall agent, host-based firewall and a port filter (Center for Internet Security, 2021). PE-IS-5 focuses on improving the authentication and control processes for users. This includes multi-factor authentication for external devices and applications, and to maintain role-based access control by determining the necessary access permissions for each role and conducting regular access control reviews to validate user privileges. These measures enhance security, authentication of users, and reduce the risk of unauthorized SIT instances.

The use of personal devices should also be mitigated with task PE-IS-6 which is to separate enterprise workspaces on personal devices. Organizations have more control over which IT instances can be utilized and that corporate data is managed and secured on personal devices. Lastly, the task PE-IS-7 addresses data encryption of sensitive files. The data can be encrypted in transit and at rest and when a data breach occurs the data will be harder to access and understand for unauthorized third parties.

5.2.2. Identify (ID)

The “Identify” phase leads to the identification and detection of SIT instances. The following two categories are needed to identify unknown IT assets within an organization, this includes asset management and activity tracking. This phase identifies the four SIT types that can occur in organizations and lists the mitigation tasks, this can be seen in Table 7.

Table 7. Mitigation tasks for SIT occurrences

SIT occurrences	Mitigation tasks
Cloud services • Unauthorized usage of personal devices to use cloud services to perform work tasks. • Accessing unauthorized cloud services using company's devices to perform work tasks. **Self-made solutions** • Unauthorized usage of personal devices to develop and use solutions to perform work tasks. • Developing and using unauthorized solutions in company's devices to perform work tasks. **Self-installed applications** • Unauthorized usage of personal devices to install and use solutions to perform work tasks. • Installing and using unauthorized solutions in company's devices to perform work tasks.	• ID-AM-1: Set up a CMDB • ID-AM-2: Implement asset discovery tools • ID-AM-3: Check system logs • ID-AM-4: Check financial administration • ID-ATR-1: Create ticketing process to management or IT service desk

Asset management (AM)

The category of asset management regarding SIT is to identify and track the organization's IT assets. The first task for an organization is ID-AM-1 which is to set up a CMDB. It is a centralized database that stores information about all the assets and configurations of the organization's IT environment. The CMDB helps to identify SIT instances because it will act as the single source of truth. By inventorying a record of all IT instances, any discrepancies or deviations can indicate instances of SIT in their network. The task ID-AM-2 supports the CMDB with implementing asset discovery tools provided by software vendors. These tools provide comprehensive visibility into the network traffic and help uncover SIT instances that may be operating outside of the organization's control. The task ID-AM-3 checks system logs for unusual activity that may occur due to the use of SIT. In addition, the organization can perform task ID-AM-4 by checking and reviewing the financial administration to identify SIT instances. By analyzing expenses, budgets, vendor invoices, and contracts potential discrepancies or unaccounted expenses can be detected. The financial examination may detect irrelevant software, overlapping licenses, and unexpected support costs that can indicate the presence of SIT.

Activity tracking and reporting (ATR)

Activity tracking and reporting mechanisms are important for an organization to help effectively identify SIT instances. The task ID-ATR-1 aims to establish a ticketing process that allows users to approach their managers or IT service desk regarding any questions or concerns related to the use of SIT. Whenever a user encounters or wants to use a SIT instance, they can submit a ticket to the IT service desk. This ticket serves as a formal record of the issue and enables both the user and the organization to track its progress until the SIT instance has been resolved. The ticketing process ensures that each reported incident is properly documented, assigned a unique identifier, and routed for investigation and ticket closure. The activity of the ticket can be tracked to show the status of the investigation and regular updates can be provided to the user to keep them informed. This enables transparency and helps build trust between users and the IT department. By tracking the activity of each SIT instance, organizations can maintain a centralized system that captures all instances of SIT and facilitates better visibility and management of the issue.

5.2.3. Evaluate (EV)

When the SIT instances are identified and detected. The “Evaluate” phase commences categorizing the SIT types, assesses the risk impact, and evaluates whether they comply with organizational and regulatory policies. This phase focuses and addresses the security risks and loss of control associated with the usage of SIT and this can be seen in Table 8.

Table 8. Mitigation tasks for security risks and control loss

Security risks	Mitigation tasks
• Potential loss of data or information leakage (§ 2.4.2.) • Weakening network security (§ 4.2.2.). • Low data confidentiality (§ 4.2.2.). • Privacy concerns of sensitive information (§ 2.4.2, § 4.2.2.). • Breach of regulatory policies and fines (§ 2.4.2.).	• EV-RC-1: Evaluate the risk impact for each SIT type • EV-RC-2: Perform vulnerability assessment • EV-RC-3: Evaluate organizational and regulatory compliance
Control loss	**Mitigation tasks**
• Loss of control in assets as systems operate outside established structures (§ 2.4.2.). • Lack of compliance with management objectives and organizational goals (§ 2.4.2.). • Breach of regulatory policies and fines (§ 2.4.2.).	• EV-RC-1: Evaluate the risk impact for each SIT type • EV-RC-2: Perform vulnerability assessment • EV-RC-3: Evaluate organizational and regulatory compliance

Risk Categorization (RC)

During the risk categorization process the SIT instances are categorized by type and the potential risk impact is assessed. The task EV-RC-1 determines the risks that are associated with each identified SIT type that is not under the control of the organization. This task focuses to address the security risk and loss of control associated with SIT and empirical research is deemed as the most important issue. The evaluation should consider factors of the sensitivity of the data, impact on business operations, and the likelihood of potential security incidents for each SIT type and instance. Cloud service providers and software vendors need to be evaluated on their security practices and reliability in terms of cloud services and installed applications. Personal devices that are not authorized should be denied and otherwise evaluated on their intentions within the organizational network. Self-made solutions are harmful because they can create backdoors and may introduce vulnerabilities and should be evaluated on coding practices and the qualifications of the individual. The task EV-RC-2 performs vulnerability assessments on the organization’s IT infrastructure and helps identify the vulnerabilities that were introduced using SIT. The assessment helps to determine the severity, impact, and likelihood of exploits of those vulnerabilities. The task EV-RC-3 evaluates the organizational and regulatory compliance of SIT instances. This evaluation ensures that the SIT instance complies with the established guidelines, security standards, and legal requirements. Non-compliant instances can be automatically denied or adjusted to bring them towards organizational compliance.

5.2.4. Analyze (AN)

The “Analyze” phase consists of activities that address the SIT risks of integration, data inconsistency, synergy loss, and inefficiency. Furthermore, this phase serves to understand the user on why they are using SIT and analyzes possible alternative tools. Table 9 outlines the SIT risks of integration, data inconsistency, synergy loss, and inefficiency and lists its mitigation tasks.

Table 9. Mitigation tasks for integration, data inconsistency, synergy loss, and inefficiency risks

Integration risks & data inconsistency	**Mitigation tasks**
• Loose coupling or a low degree of integration (§ 2.4.2.). • Damage the confidentiality, availability of services and the integrity of data (§ 4.2.2.). • Data stored on SIT instances differs from main applications (§ 4.2.2.).	• AN-UN-1: Analyze the usage patterns, volume, and users • AN-UN-2: Identify alternative tools that are compliant • AN-DM-1: Data profiling • AN-DM-2: Data mapping
Synergy loss & inefficiency	**Mitigation tasks**
• Failure to scale up or reuse beneficial local autonomous systems (§ 2.4.2.). • Wasted resources (§ 2.4.2.). • Conflicts with official systems and projects (§ 2.4.2., § 4.2.2.) • Higher and unexpected financial costs (§ 2.4.2., § 4.2.2.).	• AN-UN-1: Analyze the usage patterns, volume, and users • AN-UN-2: Identify alternative tools that are compliant • AN-DM-1: Data profiling • AN-DM-2: Data mapping

User understanding (UN)

The task AN-UN-1 is followed to analyze the volume, user patterns and identify the users. This provides valuable insights into the scale of the problem and helps prioritize actions to address the SIT instance effectively. By determining the number of users that use the SIT instance organizations can allocate appropriate resources and prioritize actions accordingly. The identification of users and usage patterns can help organizations to identify which business processes rely heavily on certain SIT solutions. The task AN-UN-2 can identify suitable alternative tools or authorized applications that can meet the specific needs of users relying on specific SIT instances. Adopting alternative tools can facilitate the transition from unauthorized instances to approved instances that minimizes integration risks, synergy loss, data inconsistencies and synergy loss.

Data management (DM)

The analysis made by task AN-UN-1 helps identify the data management capabilities to migrate, integrate, or standardize the data from SIT instances into authorized IT systems. The data cleansing activities within this category provide insights into the data landscape to eliminate inconsistencies and inefficiencies. The task AN-DM-1 consists of data profiling that assesses the content, structure, and the quality of data. It highlights the potential inconsistencies and discrepancies in SIT data. This is followed up with task AN-DM-2 data mapping that involves defining the relationships and data transformation between the different systems. The data mapping process measures the compatibility and feasibility of moving the data to authorized IT systems.

5.2.5. Respond (RE)

The "Respond" phase consists of activities to take necessary action on detected SIT instances. The information gathered from the previous phases is considered for determining the appropriate response. This phase consists of two categories that include planning and action and improvements.

Planning and action (PA)

The task RE-PA-1 determines the response planning for organizations that addresses the challenges posed by the SIT instance. The response plan should consider the risks that were identified during the previous phases and determine the acceptable level of risk. The organization should develop a plan that develops future steps if the SIT instance is accepted or denied, and whether SIT data should be moved to authorized IT systems. When the plan and future procedures are discussed then task RE-PA-2 determines whether the SIT instance is approved or denied. The decision can be documented to ensure transparency and accountability in the risk management process.

Improvements (IM)
After an organization has made the decision whether to proceed or deny a SIT instance, the organization should review and assess their existing IT landscape and identify areas of improvement. This assessment helps in evaluating whether the controls are achieving the desired outcomes. If the desired outcomes are not being met, it indicates a need for further action to align the organization's goals. The following improvement tasks can be made to address those concerns. The task RE-IM-1 involves updating security measures to address the specific risks associated with similar SIT instances. This task includes reviewing and strengthening existing information security measures to ensure the organization's environment is adequately protected. In addition, task RE-IM-2 involves updating organizational policies to explicitly address the use of SIT. This involves reviewing existing policies and creating new ones as necessary to provide clear guidelines and expectations for the usage of SIT. Task RE-IM-3 emphasizes the importance of creating awareness and providing additional training to employees. This task aims to ensure that employees have the necessary knowledge and understanding of SIT. By providing additional training, the organization can empower employees to be responsible and act secure with SIT.

5.2.6. Monitor (MO)

After the risks that are identified from prior stages and after the organization has made the final risk decision. The organization can monitor the identified risks in accordance with the response plan and take precautionary steps to SIT occurrences. The “Monitor” phase involves continuous monitoring and reviewing of risks. This phase is loosely tied to the “Identify” phase, but it focuses on detecting unauthorized instances of SIT ahead of time and automatically blocks those instances.

Event detection (ED)
The task MO-ED-1 continuously monitors the company wide network as it enables organizations to detect and respond to events caused by unauthorized SIT instances immediately. Through monitoring activities organizations can gather valuable data and generate reports that highlight the presence of SIT. Organizations can set up controls within monitoring activities to automatically block certain instances that are deemed too harmful for the organization’s IT infrastructure. By leveraging predefined rules or policies, organizations can proactively prevent the installation or usage of SIT instances.

5.3. Validation

As seen in the previous section at Figure 5 the conceptual framework is developed based on the literature research and empirical research. The phases, categories, and tasks are described to mitigate the risks of SIT. The conceptual framework is validated twice by expert interviews and two validation rounds are conducted. All participants interviewed in the first validation round can be seen in Table 4. Participant P1 and participant M1 are interviewed in the second and final validation round, due to their amount of work experience and knowledge. The validation questions for the two interview rounds are shown in Appendix D. The feedback from all the experts leads to the final version of the framework.

5.3.1. First validation round

Participant P1

Participant P1 states that the framework provides value in addressing SIT risks but highlights several areas that require clarification and improvement. He states to clarify the term of the task "*Create ticketing process to management or IT service desk* " and recommends using a more concrete and identifiable term. In the "Identify" phase he mentions that checking for system logs needs to be distinguished between network-focused analysis and host-based analysis. An emphasis is needed to distinguish the difference to avoid redundancy. Furthermore, he advises integrating the "Evaluate" phase and "Analyze" phase since they both encompass substantial elements of risk mitigation. However, he wants to exclude the task of conducting vulnerability assessments because he considers that to be conducted during a security incident. Other cybersecurity methods need to be conducted if this is deemed relevant. The emphasis lies on detecting and mitigating SIT risks and not cybersecurity incidents as other frameworks can address that. He mentions the importance of making the decision-making process explicit within the respond phase and that involves both the final risk assessment and business participation of relevant stakeholders. Participant P1 questions the distinction between the "Monitor" phase and "Identify" phase and expressed if they were not similar activities. He suggests carefully choosing words to differentiate between the two or otherwise fuse them together because of the iteration.

Participant M1

Participant M1 says that the SIT framework appears to cover all the relevant topics and attention points. He emphasizes the importance of having a strategic plan from management in the decision-making process regarding SIT. The adopted guidelines and policies are made from the strategic decision on whether to allow or disallow SIT instances. In addition, he mentions that the task "*Create ticketing process to management or IT service desk*" should be part of the "Prevent" phase, as it functions to require users to follow proper request procedures that is part of IT governance. Participant M1 notes the importance of analyzing network traffic and logs during the evaluation phase and proposed switching the order of the evaluate and analyze phases to better reflect the process of analyzing data and then evaluating the risks. Participant M1 notes that the "Respond" phase is deemed acceptable, but that the improvements category can be excluded because of the iteration back to the prevent phase where the improvements can directly be made on governance, human resource management and information security. He mentions that within the "Respond" phase an additional task can be highlighted, which is the communication aspect in which every stakeholder is informed about the final decision. He shares that the overall framework could be useful if the tasks within the framework are regularly updated and that it always differs per organization.

Participant M2

Participant M2 suggests that a SIT strategy needs to be formulated before the necessary policies and guidelines can be created. He further states that the "Monitor" phase and "Prevent" phase seems to be more aligned with each other because of it being a strategic process and not an operational process. He argues that continuous and periodic monitoring provides insights into the effectiveness of a risk mitigation strategy and helps the effectiveness of the overall decision-making process. M2 states that the developed framework shares similarities and provides benefits of alignment with existing cybersecurity frameworks. He remarks that it provides a unique insight for clients to address SIT concerns. He states that it is insightful that there is a distinction made between the evaluate and analyze phase to address the different SIT risks.

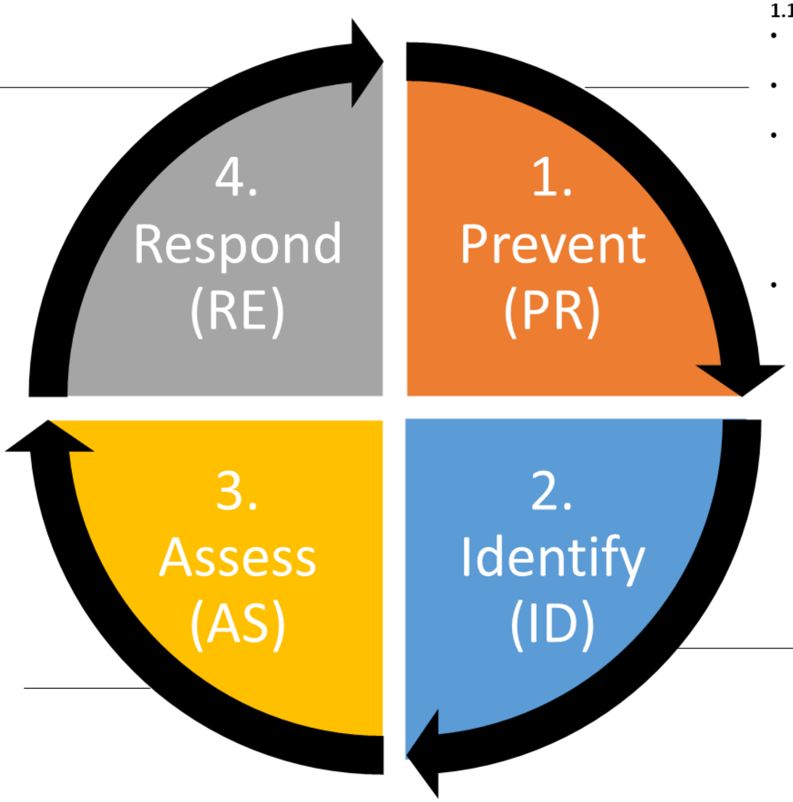
Participant SE2

Participant SE2 argues that a strategy needs to be formulated before addressing and creating policy and procedures regarding SIT risks. He expresses that preventing the use of SIT is not always necessary but understands that a policy serves as a suitable baseline. Moreover, he states that the "Analyze" phase regarding data profiling and data mapping can be labeled under one task named data cleansing. He mentions the task "Perform vulnerability assessment" should occur in the "Monitor" phase ensuring that any vulnerabilities caused by SIT are continuously monitored. Participant SE2 states that the phases and tasks within the developed framework are useful in mitigating SIT risks.

5.3.2. First validation adjustments

The feedback provided by the participants from the first validation leads to the adjustments for the framework. Figure 6 outlines the second version of the framework that was provided by the feedback from the first validation round. The adjustments from the first validation round are as follows:

- The task PR-GV-1: "Formulate" SIT strategy is newly created and stated as the first task, and it is to address the decision-making process of organizations to mitigate SIT risks.
- The task PR-GV-4: "Create awareness and facilitate training" is renamed to "Maintain awareness and facilitate training", due to the iterative process of the framework.
- The task ID-ATR-1 is renamed from "Create ticketing process to management" to PR-GV-5 "IT service desk". It is moved from the "Identify" phase to the "Prevent" phase, due to it being a management procedure.
- The category "Activity tracking and reporting" is removed because it contains no more tasks.
- The "Evaluate" phase and "Analyze" phase are merged into one phase named the "Assess" phase, for better comprehension and simplification purposes.
- All tasks within the "Evaluate" phase and "Analyze" phase are renamed from "EV" and "AN" to "AS", because it now resides in the "Assess" phase.
- The tasks AN-DM-1 and AN-DM-2 are merged into one task named AS-DM-1: "Data cleansing", for better comprehension and simplification purposes.
- The task EV-RC-2: "Perform vulnerability assessment" is removed, because it addresses incident response management and not risk management.
- The task RE-PA-3: "Communicate decision" in the "Respond" phase is newly created, to inform every stakeholder about the final decision.
- The category "Improvements" and its corresponding tasks RE-IM-1, RE-IM-2, RE-IM-3 within the "Respond" phase are removed, due to the iterative process of the framework.
- The "Monitor" phase and the task MO-ED-1 is removed, due to the iterative process of the framework.



1.1 Governance (GV)

- PR-GV-1: Formulate SIT risk strategy
- PR-GV-2: Policies and procedures
- PR-GV-3: Communication and collaboration
  PR-GV-4: Maintain awareness and facilitate training
- PR-GV-5: IT service management

1.2 Information Security (IS)

- PE-IS-1: Whitelist authorized software
- PE-IS-2: Implement DNS and URL filters
- PE-IS-3: Restrict unapproved browser and email client extensions
- PE-IS-4: Configurate firewall settings
- PE-IS-5: Authentication and access control
- PE-IS-6: Separate enterprise workspaces on personal devices
- PE-IS-7: Data encryption

2.1 Asset management (AM)

- ID-AM-1: Set up a CMDB
- ID-AM-2: Implement asset discovery tools
- ID-AM-3: Check system logs
- ID-AM-4: Check financial administration

3.1 Risk categorization (RC)

- AS-RC-1: Evaluate the risk impact for each SIT type
- AS-RC-2: Evaluate organizational and regulatory compliance

3.2. User understanding (UN)

- AS-UN-1: Analyze the usage patterns, volume, and users
- AS-UN-2: Identify alternative tools

3.3. Data management (DM)

- AS-DM-1: Data cleansing

4.1 Planning and action (PA)

- RE-PA-1: Response planning
- RE-PA-2: Approve or deny SIT instance
- RE-PA-3: Communicate decision

Figure 6. Second version SIT risk management framework

5.3.3. Second validation round

Participant P1

Participant P1 argues that the task ID-AM-3 “Check system logs” can be extended to encompass the analysis of system logs from end-user devices and firewalls, which expands the framework’s monitoring capabilities. Furthermore, he suggests adding an extra task to the “Identify” phase, which is to detect SIT instances based on security events. This task functions as a continuous monitoring activity that actively checks the security implementations and assesses the status of IT assets. He is positive that the framework provides a clear and accessible environment for organizations, as they can use the resource without completely replacing their existing measures. In addition, he appreciates the clarity and simplicity of the framework for its usability and ease of interpretability.

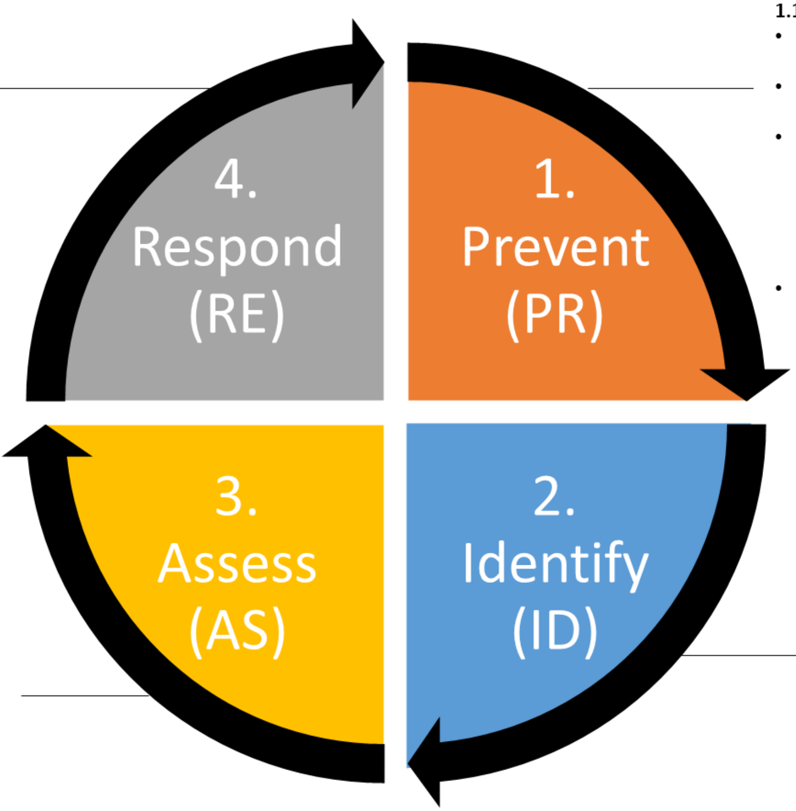
Participant M1

Participant M1 expresses satisfaction with the adjusted framework, particularly highlighting improvements in the rearrangements of the tasks, simplification of the phases, and the logical structure of the framework. He argues that the approach to SIT risk assessment, starting with what is already known and then identifying unknown instances is important. He suggests rearranging the tasks in the “Identify” phase and proposes to move task ID-AM-4 before task ID-AM-2, because task ID-AM-4 identifies existing SIT instances with checking the financial administration that are known in BUs and not the IT department. He continues by saying that the current tasks of ID-AM-2 and ID-AM-3 identifies, and addresses SIT instances that are unknown to the BUs and IT department and should follow-up after task ID-AM-4. He is overall positive about the framework as it can serve as a logical and useful tool for managing SIT.

5.3.4. Second validation adjustments

The second version of the framework is adjusted based on the feedback from the participants in the second validation round. The final adjustments resulting from this feedback are summarized in Figure 7 that presents the final version of the framework. The final adjustments made during the second validation round include the following:

- The task ID-AM-3: “Check system logs” is renamed and extended to analyze and detect system logs from end-user devices and firewalls.
- The task ID-AM-5: “Detect SIT based on security events” in the “Identify” phase is newly created, to continuously check security implementations and status of IT assets.
- The task ID-AM-4 is moved and renamed to task ID-AM-2, subsequently task ID-AM-2 and task-ID-AM-3 are renamed to task ID-AM-3 and task ID-AM-4. This is because checking financial administration identifies SIT instances that are known in the BUs, and the other tasks identifies SIT instances that are unknown to both the IT department and BUs.



4.1 Planning and action (PA)

- RE-PA-1: Response planning
- RE-PA-2: Approve or deny SIT instance
- RE-PA-3: Communicate decision

1.1 Governance (GV)

- PR-GV-1: Formulate SIT risk strategy
- PR-GV-2: Policies and procedures
- PR-GV-3: Communication and collaboration
  PR-GV-4: Maintain awareness and facilitate training
- PR-GV-5: IT service management

1.2 Information Security (IS)

- PE-IS-1: Whitelist authorized software
- PE-IS-2: Implement DNS and URL filters
- PE-IS-3: Restrict unapproved browser and email client extensions
- PE-IS-4: Configurate firewall settings
- PE-IS-5: Authentication and access control
- PE-IS-6: Separate enterprise workspaces on personal devices
- PE-IS-7: Data encryption

3.1 Risk categorization (RC)

- AS-RC-1: Evaluate the risk impact for each SIT type
- AS-RC-2: Evaluate organizational and regulatory compliance

3.2. User understanding (UN)

- AS-UN-1: Analyze the usage patterns, volume, and users
- AS-UN-2: Identify alternative tools

3.3. Data management (DM)

- AS-DM-1: Data cleansing

2.1 Asset management (AM)

- ID-AM-1: Set up a CMDB
- ID-AM-2: Check financial administration
- ID-AM-3: Implement asset discovery tools
- ID-AM-4: Check system logs from end-user devices and firewalls
- ID-AM-5: Detect SIT based on security events

Figure 7. Final version SIT risk management framework

6. Discussion

In this chapter, the main findings are discussed in Section 6.1. Section 6.2. outlines the research implications with the seven design science research guidelines (Hevner et al. 2004) as it reviews the overall research quality from this research. Section 6.3. discusses the research contributions in terms of academical and managerial relevance. The last section explains the research limitations and elaborates on recommendations for future research.

6.1. Main findings

The main findings of the research help answer the main research question and sub-questions. The research aims to answer the main research question: *"How can an IT risk framework be successfully developed to effectively identify, assess and manage SIT risks within organizations?"*. Through literature research, the first sub-question: "What are the characteristics of SIT?" is answered by identifying the determinants, effects, and types of SIT. These characteristics of SIT were additionally mentioned through interviews with risk management experts.

The SIT determinants are categorized in enablers, motivators, and missing barriers (Klotz et al., 2019). Enablers are distinguished between technical accessibility and IT user competence. The findings suggest that technical accessibility plays a significant role in driving the adoption of SIT tools among employees. Half of the participants emphasized the availability and convenience of these tools provided by external parties, leading employees to seek out alternatives that address their productivity needs. This highlights the importance of considering the accessibility factor when examining the prevalence of SIT within organizations. Moreover, IT user competence was acknowledged by roughly half of the participants as employees are becoming more tech savvy and actively seek more efficient and productive solutions independently. The biggest culprit is that employees want to save time and effort in their work processes, and do not concern using tools provided by the organization or external parties. The findings suggest that employees are inclined to explore alternative tools driven by their own motivation to enhance productivity.

The determinants that motivate the adoption of SIT include a poor business-IT alignment and the shortcomings of IT systems. Half of the participants deemed that poor business-IT alignment can enable the prevalence of SIT. The findings suggest that this misalignment of responsibilities between the BUs and IT departments can create a divide in determining ownership and management of SIT. It is noted that participants find that over the years the BUs are becoming more and solely responsible in managing the organization's IT tools. It is stated that this misalignment between BUs and IT departments also hampers budget allocation and resource planning, and that better collaboration and communication is needed. Additionally, the shortcomings of IT systems are raised as a concern by roughly half of the participants. Participants observed that employees often turn to SIT when they encounter difficulties or limitations with the tools provided by the organization. Issues with usability, inefficiency, and time constraints were cited as common reasons for employees to explore alternative tools. This highlights the importance of providing user-friendly and efficient IT systems to mitigate the risks associated with SIT.

Missing barriers serve as a determinant for SIT and it includes a misalignment of IT governance and a lack of awareness. The findings of the study show that most participants identified that the misalignment of IT governance within organizations can significantly influence the adoption of SIT. Participants noted that organizations do not consider SIT as a high IT risk and consequently do not prioritize managing SIT-related risks. This is made clear by another participant that organizations do not pay much attention to its presence within their environments. The findings suggest that organizations lack a comprehensive understanding of their total inventory, as it makes it more challenging to determine if existing security controls are justified. A participant noted that identifying their total network is more focused on detecting vulnerabilities and misconfigurations, than actively monitoring for SIT risk instances. Moreover, in terms of IT governance the study shows that organizations may face a lack of clarity and compliance in end-user policies regarding SIT. As policies fail to provide clear guidelines or explicit prohibitions in the use of SIT. This ambiguity can lead to uncertainty among employees regarding whether their actions align with organizational policies. In addition, the research findings suggest that a lack of awareness among employees exists regarding the risks associated with SIT and existing IT policies. Participants emphasized that user awareness plays an important role in dealing with the risks of SIT. Another participant mentioned that employees do not recognize instances of SIT, as they perceive those tools as part of the organization's IT landscape.

Negative SIT risk effects include security risks, integration risks and data inconsistency, control loss, synergy loss and inefficiency. In terms of negative SIT risks almost all participants stated that security risk is the most important factor due to the risks of data leakage and network vulnerability. The participants mention that third-party file transfer tools are a common risk in terms of data security and privacy. This leads to loss of control of data, as participants noted that limited security controls exist within organizations because SIT instances are often unknown or unmanaged. This lack of control prevents organizations from implementing necessary security measures and maintaining a holistic overview of their IT landscape. The use of cloud services raises further concerns, as organizations may not have full knowledge of where their information is stored and for how long.

Almost all participants raise concern over synergy loss and inefficiency risks as it is found out that the presence of multiple systems for one business process leads to a lack of clarity on which data source is the most accurate. This ambiguity can result in financial costs and inefficiencies for the organization. It is also noted that challenges lie in determining whether to deny or approve a SIT solution that gains significant adoption within the organization. As the organization must consider security, privacy, and financial considerations in its decision-making processes. Half of the participants mentioned the integration risks and data inconsistency issues caused by SIT. The concern is that there is inadequate synchronization of data because it is entered into separate systems. This can cause problems during auditing processes and hinders the reliability of information because the data is incomplete.

The different types of SIT instances are cloud services, installed applications, self-made solutions, personal devices. The findings of the different types of SIT and its risk impact varied by participants. As each type of SIT carries its own risks, it is notable that participants generally considered self-installed applications and unauthorized cloud services as the most severe. Self-installed applications introduce direct vulnerabilities into the network, while unauthorized cloud services pose challenges related to data ownership and control. Personal devices and self-made solutions were also regarded as significant risks, emphasizing the importance of addressing security concerns associated with personal devices and ensuring proper coding and maintenance of internally developed solutions.

The second sub-question is also answered through literature research and empirical research*: "What are the current available methods and frameworks that address SIT?"*. The literature research explained that there exists no specific risk management framework that can manage the risks of SIT. The literature study outlined the three most popular risk management frameworks such as ISO/IEC, COBIT, and NIST as it explores each framework's management approach in terms of control, governance, risk, and compliance.

The research findings also dictate that most participants expressed unawareness of any dedicated frameworks or methods that can deal with SIT. Some mention that SIT is embedded within existing risk frameworks but feel that these frameworks could be improved to better address the risks associated with SIT. The participants stressed that more detailed guidance and a comprehensive framework that explicitly addresses the challenges and risks associated with SIT is needed.

The third sub-question is answered through empirical research and is stated as follows: *"What are the requirements of risk management experts to develop a SIT risk management framework?".* In developing a SIT risk management framework semi-structured individual interviews were held with risk management experts. The answers from the experts were analyzed through a thematic analysis and notable framework phases and mitigation tasks were identified. The developed framework inspired by the ISO/IEC, COBIT, and NIST frameworks follows an iterative approach and consists of four phases: prevent, identify, assess, and respond. The prevent phase aims to prevent the occurrence of SIT determinants by addressing the necessary criteria to mitigate the associated risks. Subsequently, the identify phase helps organizations identify unknown IT assets within their infrastructure and identifies the SIT types. Following the identification of SIT instances, the assess phase commences. This phase categorizes the types of SIT and assesses each of the SIT risks in terms of risk impact, compliance, data management, and identifying alternative tools. Finally, the respond phase involves taking necessary actions on the detected SIT instance. The information gathered from the previous phases is utilized to determine the appropriate response.

The final sub-question is answered through validation interviews with risk management experts: *"To what extent can the SIT risk management framework be utilized by organizations?".* The framework aims to provide a structured and comprehensive approach for organizations to manage the risks associated with SIT. Through expert interviews participants have responded positively to the development of the framework. The participants highlighted that the second version could be proven useful in real-world scenarios. However, due to time constraints the participants were not asked about their opinions on the final version of the framework. In addition, the research findings indicated that numerous companies fail to allocate sufficient resources and time towards identifying suspicious network traffic, with challenges arising in the context of SIT instances. The participants mentioned that SIT is often not considered a security priority for organizations. This outlines that SIT needs to be prioritized within organizational agendas before organizations are motivated to allocate the resources for the developed framework towards the detection and management of SIT instances.

6.2. Implications

This section discusses the research implications in developing the framework. The seven guidelines of Hevner et. al (2004) are used to evaluate the quality of the research as shown in Table 10.

Table 10. Design science research guidelines (Hevner et al., 2004)

Guideline	Description
1. Design as an artefact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2. Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.

3. Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4. Research contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
5. Research rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6. Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
7. Communication of research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

The above research guidelines are applied in this research and leads to the following implications:

Guideline 1: Design as artifact
The result of this research is to create a viable artifact in the form of a SIT risk management framework. Through literature research and empirical research, the key requirements, challenges, and best practices related to managing SIT are identified. As a result, the framework integrates these findings into a cohesive and practical solution, providing guidance to organizations seeking to address the risks associated with SIT.

Guideline 2: Problem relevance
SIT is a growing concern in recent years, as most organizations are compromised due to the use of SIT instances. This important business challenge has been elaborated in Chapter 1 that discusses the problem indication and problem statement. Therefore, given the limitations of current management frameworks, the hidden nature of SIT instances, the lack of risk assessments, and the incomplete understanding of employee utilization, makes it clear that a dedicated SIT risk management framework is needed.

Guideline 3: Design evaluation
During the development and evaluation of the artifact, two validation rounds were conducted that involved a total of six participants with expertise in risk management and extensive knowledge of SIT. The participants for both validation rounds were selected based on purposive sampling. Participants were chosen based on the most relevant expertise and knowledge regarding SIT and risk management. They were given sufficient time to review and analyze the artifact, evaluating its applicability and effectiveness in addressing the risks of SIT. The framework was adjusted based on the expert's evaluation of the artifact after both validation rounds. The feedback facilitated iterative improvements and ultimately enhanced the overall quality and effectiveness of the final version of the framework.

Guideline 4: Research contributions
The contribution of this research is that it provides a robust SIT risk management framework that provides a comprehensive and practical approach for managing SIT. It is developed by the insights from risk management experts and current literature. In terms of existing frameworks, none of the frameworks

addresses the risks of SIT specifically and therefore the developed framework fills the gap and contributes to new knowledge in the academic field. Furthermore, the framework offers guidelines and recommendations that organizations can use to proactively address SIT risks.

Guideline 5: Research rigor
In the realm of design science research, rigorous methods are essential for both constructing and evaluating the designed artifact (Hevner et al., 2004). The SIT risk management framework is based on existing risk management frameworks and other sources found in the literature review. In addition, nine risk management expert was interviewed to obtain their opinion regarding SIT to create the initial draft of the SIT framework. Furthermore, two validation rounds were held where feedback was obtained for the developed SIT risk management framework. The validation process with the experts helped to ensure the resilience and reliability of the SIT risk management framework. Through multiple iterations and incorporating these inputs, the final version of the SIT risk management framework was developed. By developing a SIT risk management framework, organizations can develop a deeper understanding of SIT risks and enable them to integrate these insights into controllable actions.

Guideline 6: Design as a search process
In this research, the developed SIT risk management framework is a dynamic process characterized by continuous iterations and refinements. To identify the key requirements, semi-structed interviews were held with nine risk management experts to obtain their opinions regarding SIT risk and management, which informed the initial version of the SIT risk management framework. Through validation interviews and expert feedback, the SIT risk management framework was refined and improved, incorporating additional insights, and ensuring its usability and effectiveness. This interactive search process enabled the development of the final SIT risk management framework.

Guideline 7: Communication of research
The developed framework is specifically designed for IT risk management and cybersecurity experts who possess in-depth knowledge and understanding of SIT. These professionals play a critical role in ensuring the security and integrity of organizational IT infrastructure. The framework supports the organizational decision-making processes as it can assist in resource allocation and enables effective governance of SIT risks. Furthermore, the framework provides security measures and technical solutions to identify and mitigate SIT risks. The research aims to provide both technological and managerial oriented audiences with a comprehensive tool that enables them to effectively manage SIT risks in their respective organizations.

6.3. Contributions

This section elaborates the developed framework from this research and its academic and managerial contributions to empower organizations in navigating the complexities of managing SIT instances.

Academic relevance
The current literature and as evidenced by empirical research, the subject of risk management in SIT is limited. During the research all participants mentioned that there exist to their knowledge no SIT risk management framework. The research findings based on literature research and empirical research provide a risk management framework that can manage the risks of SIT. This includes identifying the underlying causes and motivations behind SIT adoption, exploring the potential risks it poses to organizations, and examining the impact of managing these risks. This research is one of the few empirical studies that aims to manage the risks of SIT by developing a practical framework. It extends the existing

identification and evaluation steps of SIT (Rentrop & Zimmermann, 2012a) as the study explores mitigation tasks for SIT determinants and SIT risks and integrates it towards a risk management framework. In addition, the research contributes to existing risk management frameworks as stated that their approaches are not easy to carry out in practice (Tøndel et al., 2014). This research provides a practical framework as participants noted its ease of interpretability for organizations to manage SIT risks. Furthermore, existing risk management frameworks outlines that the responsibility to manage privacy and security belongs to the top management team (Taherdoost, 2022). However, this study outlines that in terms of SIT responsibility predominantly lies with individual users and not solely top management. This research outlines that top management influences control over IT systems, tools, and its organizational culture and that it can affect the attitude and behavior of employees in using SIT. The developed framework provides new tools and insights to effectively promote better IT management to mitigate the threats of SIT. As it provides stepwise methodology in addressing SIT risks within organizations. The result of this research proves a practical and flexible framework designed by experts in the field, that contributes to the existing academic landscape of managing SIT risks.

Managerial relevance

The developed SIT risk management framework offers valuable managerial insight and practical guidelines for organizations to proactively identify, assess and mitigate SIT risks. IT managers can leverage the SIT risk management framework to enhance their decision-making process, allocate resources efficiently, and develop strategies to address the specific needs and contexts of their organizations. Additionally, this managerial contribution fosters a proactive risk management culture within organizations, enabling them to align their IT governance structures, policies and controls with the topic of SIT. By adopting this developed framework organizations can enhance their overall risk posture, strengthen their IT governance structures, and protect their digital assets in the evolving technological landscape.

6.4. Limitations and future research

During the research of developing a SIT risk management framework, several limitations were encountered. The lack of previous research studies on the topic of SIT poses a challenge as there may be limited existing knowledge regarding SIT risk management to draw upon. This requires more reliance on primary data collection and may lead to a less comprehensive understanding of the subject matter. However, the findings from this research can enable future research to focus on measuring the effectiveness of each mitigation task within the SIT risk management framework.

Conducting the study within four months limited the scope of data collection, analysis, and the overall development of the framework. This limited timeframe means that the developed artifact could not be tested on a real case by consultants. To compensate for this, validation took place by seeking consultants' opinions on whether they could envision using the framework for their client cases. To enhance the validity and practical applicability of the developed framework, future research should aim to conduct case studies where the framework can be applied and tested in real-world SIT risk management scenarios.

Moreover, the sample of risk management experts that were interviewed consisted of only nine participants from a big four firm. To overcome limitations related to sample size and generalizability, future research should aim to include a larger and more diverse participant pool from various organizations, industry sectors, and geographical locations.

This study focused more on SIT that is related to productivity tools used by individuals, but shadow internet of things (IoT) is also gaining more traction in causing security issues within organizations. As this relates to IoT devices that have unauthorized access to an organizational network. Future research can be conducted to identify shadow IoT risks, its mitigations, and integrate it into the developed SIT risk framework.

In addition, future research can also address the gap in motivation among organizations to allocate resources towards the detection and management of SIT instances. This call for future research includes examining the challenges faced by organizations, such as competing priorities for information security, limited budgets, and exploring the lack of understanding regarding the dangers of SIT.

All the above considerations for future research would provide valuable insights into the effectiveness, practicality, and adaptability of the framework in diverse organizational contexts.

7. Conclusion

This research explored the feasibility of creating an IT risk management framework for organizations and consultants that can mitigate and manage SIT risks. The need for the development of the framework is that most organizations are compromised in their security due to usage of SIT, and of recent years there is a significant increase of cybersecurity attacks.

Design science research was carried out and consisted of literature research and empirical research. The literature research identified the SIT determinants, SIT risks, SIT types, and current risk management frameworks to understand the whole scope of the problem. The literature research helped to identify the research gaps that can be addressed during the empirical research. The empirical research that was conducted helped to create the final artifact in the form of a framework. Semi-structured individual interviews were held with several risk management experts to identify the requirements for the framework, the data was analyzed by a thematic analysis. Afterwards two validation rounds were held that helped design the final iteration of the framework. The final SIT risk framework outlines the following four phases: “Prevent”, “Identify”, “Assess”, and “Respond”. Each phase manages the different aspects and elements of SIT in terms of determinants, risks, and types. The last phase determines the appropriate action and response on detected SIT instances that is based on the information gathered from previous phases.

This study can be considered as one of the first to integrate the characteristics of SIT into a practical risk management framework. As existing literature indicate a limited understanding of risk management in SIT. This research fills this gap by developing a practical risk management framework specifically designed to address the risks associated with SIT. The framework identifies the underlying causes and motivations behind SIT adoption, explores potential risks, and examines the impact of managing these risks. This study sheds light on the shared responsibility of individual users in the context of SIT and it allows organizations to adopt a more holistic approach to SIT risk management. It is a practical and flexible solution designed by experts in the field, making a valuable contribution to the existing academic and managerial landscape of managing SIT risks.

In conclusion, this research advances the understanding of SIT risk management by offering a comprehensive framework that addresses the limitations of existing approaches. It provides organizations with a practical toolset to identify, assess, and mitigate the risks associated with SIT.

References

Afreen, A. (2017). Bring your own device (BYOD) in higher education: Opportunities and challenges. *International Journal of Emerging Trends & Technology in Computer Science*, *3*(1), 233–236.

Al-Ahmad, W., & Mohammad, B. (2012). Can a single security framework address information security risks adequately. *International Journal of Digital Information and Wireless Communications*, *2*(3), 222–230. https://sdiwc.net/digital-library/can-a-single-security-framework-address-information-security-risks-adequately.html

Alter, S. (2014). Theory of Workarounds. *Communications of the Association for Information Systems*, *34*. https://doi.org/10.17705/1cais.03455

Azad, B., & King, N. (2012). Institutionalized computer workaround practices in a Mediterranean country: an examination of two organizations. *European Journal of Information Systems*, *21*(4), 358–372. https://doi.org/10.1057/ejis.2011.48

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. *Communications of the ACM*, *52*(2), 124–129. https://doi.org/10.1145/1461928.1461960

Behrens, S., & Sedera, W. (2004). Why do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study. *Pacific Asia Conference on Information Systems*, 136.

Beimborn, D., & Palitza, M. (2013). Enterprise App Stores for Mobile Applications : Development of a Benefits Framework. *Americas Conference on Information Systems*.

Bendor-Samuel, P. (2017). *How To Eliminate Enterprise Shadow IT | Sherpas In Blue Shirts*. Everest Group. https://www.everestgrp.com/2017-04-eliminate-enterprise-shadow-sherpas-blue-shirts-39459.html/

Berente, N., Yoo, Y., & Lyytinen, K. (2008). Alignment or Drift? Loose Coupling over Time in NASA's ERP Implementation. *International Conference on Information Systems*, 180.

Boudreau, M., & Robey, D. (2005). Enacting Integrated Information Technology: A Human Agency Perspective. *Organization Science*, *16*(1), 3–18. https://doi.org/10.1287/orsc.1040.0103

Bounagui, Y., Mezrioui, A., & Hafiddi, H. (2019). Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models. *Computer Standards & Interfaces*, *62*, 98–118. https://doi.org/10.1016/j.csi.2018.09.001

Buchwald, A., & Urbach, N. (2012). Exploring the Role of Un-Enacted Projects in IT Project Portfolio Management. *International Conference on Information Systems*.

Center for Internet Security. (2021). *CIS Critical Security Controls Version 8*. CIS. https://www.cisecurity.org/controls/v8

Chua, C. E. H., Storey, V. C., & Chen, L. (2014). Central IT or Shadow IT? Factors Shaping Users' Decision to Go Rogue With IT. *International Conference on Information Systems*. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1314&context=icis2014

Cisco Umbrella. (2021). *Secure Shadow IT: Protect your digital transformation with Cisco Umbrella*. https://learn-cloudsecurity.cisco.com/umbrella-resources/umbrella/secure-shadow-it#page=1

Core. (2021). *2020 was a year of change: how ready was the market, and how ready were you?* https://www.core.co.uk/2020-was-a-year-of-change-a-core-research-report

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Cybersecurity Ventures. (2022). *2022 Official Cybercrime Report*. https://www.esentire.com/resources/library/2022-official-cybercrime-report

Davison, R. M., & Ou, C. X. (2018). Subverting organizational IS policy with feral systems: a case in China. *Industrial Management and Data Systems*, *118*(3), 570–588. https://doi.org/10.1108/imds-04-2017-0153

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

Fürstenau, D., & Rothe, H. (2014). Shadow IT systems: discerning the good and the evil. In *European Conference on Information Systems*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1197&context=ecis2014

Fürstenau, D., Rothe, H., & Sandner, M. (2017). Shadow Systems, Risk, and Shifting Power Relations in Organizations. *Communications of the Association for Information Systems*, *41*, 43–61. https://doi.org/10.17705/1cais.04103

Garbutt, G. (2022). How Shadow IT Can Keep Compliance Efforts In The Dark. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2022/07/19/how-shadow-it-can-keep-compliance-efforts-in-the-dark/?sh=7bd56a962d10

GDPR. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Gehrmann, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. *Navus: Revista De Gestão E Tecnologia*, *2*(2), 66–77. https://doi.org/10.22279/navus.2012.v2n2.p66-77.77

Goosen, R., & Rudman, R. J. (2013). An Integrated Framework To Implement It Governance Principles At A Strategic And Operational Level For Medium-To Large-Sized South African Businesses. *International Business & Economics Research Journal*, *12*(7), 835. https://doi.org/10.19030/iber.v12i7.7972

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT Consumerization and the Transformation of IT Governance. *Management Information Systems Quarterly*, *42*(4), 1225–1253. https://doi.org/10.25300/misq/2018/13703

Györy, A. a. B., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. *European Conference on Information Systems*, 222. http://aisel.aisnet.org/ecis2012/222/

Haag, S. (2015). Appearance of Dark Clouds? - An Empirical Analysis of Users' Shadow Sourcing of Cloud Services. *RePEc: Research Papers in Economics*.

Haag, S., & Eckhardt, A. (2014). Normalizing the Shadows – The Role of Symbolic Models for Individuals' Shadow IT Usage. *Research Papers in Economics*. http://econpapers.repec.org/paper/darwpaper/82696.htm

Haag, S., & Eckhardt, A. (2017). Shadow IT. *Business &Amp; Information Systems Engineering*, *59*(6), 469–473. https://doi.org/10.1007/s12599-017-0497-x

Haag, S., Eckhardt, A., & Bozoyan, C. (2015). Are Shadow System Users the Better IS Users? - Insights of a Lab Experiment. *Publications of Darmstadt Technical University, Institute for Business Studies (BWL)*.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management. *DOAJ (DOAJ: Directory of Open Access Journals)*, *4*(4), 27–47. https://doi.org/10.12821/ijispm040402

Hevner, A. R., & Chatterjee, S. (2010). Design Research in Information Systems. *Springer eBooks*. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, March, Park, & Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Houghton, L., & Kerr, D. (2006). A study into the creation of feral information systems as a response to an ERP implementation within the supply chain of a large government-owned corporation. *International Journal of Internet and Enterprise Management*, *4*(2), 135. https://doi.org/10.1504/ijiem.2006.010239

Huber, M., Zimmermann, S., Rentrop, C., & Felden, C. (2017). The Influence of Shadow IT Systems on Enterprise Architecture Management Concerns. *Lecture Notes in Business Information Processing*, 461–477. https://doi.org/10.1007/978-3-319-65930-5_37

Huuskonen, S., & Vakkari, P. (2013). "I Did It My Way": Social workers as secondary designers of a client information system. *Information Processing and Management*, *49*(1), 380–391. https://doi.org/10.1016/j.ipm.2012.05.003

IBM. (2023). *Cost of a data breach 2022*. https://www.ibm.com/reports/data-breach

Inside Track Staff. (2023). *Shining a light on how Microsoft manages Shadow IT*. Microsoft. https://www.microsoft.com/insidetrack/blog/shining-a-light-on-how-microsoft-manages-shadow-it/

ISACA. (2018a). *COBIT 2019 Framework: Governance and Management Objectives*.

ISACA. (2018b). *COBIT 2019 Framework: Introduction and Methodology*.

ISO. (2022). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks: ISO/IEC 27005:2022*. https://www.iso.org/standard/80585.html

Joint Task Force. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy: NIST Special Publication 800-37 Revision 2. *NIST*. https://doi.org/10.6028/nist.sp.800-37r2

Jones, D. R., Behrens, S., Jamieson, K., & Tansley, E. (2004). The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation. *Association for Information Systems*, *96*.

Kerr, D., & Houghton, L. (2010). Just in time or Just in case: A Case study on the impact of context in ERP implementations. *Australasian Journal of Information Systems*, *16*(2). https://doi.org/10.3127/ajis.v16i2.549

Kerr, D., Houghton, L., & Burgess, K. (2007). Power Relationships that Lead to the Development of Feral Systems. *Australasian Journal of Information Systems*, *14*(2). https://doi.org/10.3127/ajis.v14i2.473

Klotz, S., Kopper, A., Westner, M., & Strahringer, S. (2019). Causing factors, outcomes, and governance of Shadow IT and business-managed IT: a systematic literature review. *International Journal of Information Systems and Project Management*, *7*(1), 15–43. https://doi.org/10.12821/ijispm070102

Kopper, A., & Westner, M. (2016a). Deriving a framework for causes, consequences, and governance of shadow IT from literature. *MKWI 2016 Proceedings*, 1687–1698.

Kopper, A., & Westner, M. (2016b). Towards a Taxonomy for Shadow IT. *Americas Conference on Information Systems*.

Kopper, A., Westner, M., & Strahringer, S. (2020). From Shadow IT to Business-managed IT: a qualitative comparative analysis to determine configurations for successful management of IT by business entities. *Information Systems and e-Business Management*, *18*(2), 209–257. https://doi.org/10.1007/s10257-020-00472-6

Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud & Security*, *2017*(6), 5–8. https://doi.org/10.1016/s1361-3723(17)30050-7

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers &Amp; Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Liang, H., Xue, Y., & Wu, L. (2013). Ensuring Employees' IT Compliance: Carrot or Stick? *Information Systems Research*, *24*(2), 279–294. https://doi.org/10.1287/isre.1120.0427

Lyytinen, K., & Newman, M. C. (2015). A tale of two coalitions - marginalising the users while successfully implementing an enterprise resource planning system. *Information Systems Journal*, *25*(2), 71–101. https://doi.org/10.1111/isj.12044

Mallmann, G. L., Maçada, A. C. G., & Oliveira, M. (2018). The influence of shadow IT usage on knowledge sharing. *Business Information Review*, *35*(1), 17–28. https://doi.org/10.1177/0266382118760143

Myers, N., Starliper, M. W., Summers, S. A., & Wood, D. A. (2017). The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making. *Accounting Horizons*, *31*(3), 105–123. https://doi.org/10.2308/acch-51737

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://doi.org/10.6028/nist.cswp.04162018

Netskope Threat Labs. (2021). *Cloud and Threat Report - July 2021 Edition*. https://www.netskope.com/lp-cloud-and-threat-report-july-2021-edition-web

Ozkan, N., Bulut, K. N., Gok, M. S., & Ozer, G. (2021). Controlling Shadow IT: Case Study from a Turkish Bank. *2021 6th International Conference on Computer Science and Engineering (UBMK)*. https://doi.org/10.1109/ubmk52708.2021.9558944

Peltier, T. R. (2017). *Information Security Fundamentals, Second Edition*. Auerbach Publications.

Puhakainen, P., & Siponen, M. T. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *Management Information Systems Quarterly*, *34*(4), 757. https://doi.org/10.2307/25750704

Raković, L., Sakal, M., Matković, & Marić, M. (2020). Shadow IT – Systematic Literature Review. *Information Technology and Control*, *49*(1), 144–160. https://doi.org/10.5755/j01.itc.49.1.23801

Randori. (2023). *The State of Attack Surface Management 2022*. https://www.randori.com/reports/the-state-of-attack-surface-management-2022/

Recker, J. C. (2021). Scientific Research in Information Systems. *Progress in IS*. https://doi.org/10.1007/978-3-030-85436-2

Reddy, R. (2021). Shadow IT in the SaaS World - A Complete Guide. *Zluri*. https://www.zluri.com/blog/shadow-it/

Rentrop, C., & Zimmermann. (2012a). Shadow IT: Management and Control of unofficial IT. *ICDS 2012 : The Sixth International Conference on Digital Society*, 98–102.

Rentrop, C., & Zimmermann, S. (2012b). Shadow IT evaluation model. *Federated Conference on Computer Science and Information Systems (FedCSIS)*, 1023–1027.

Robinson, O. J. (2014). Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide. *Qualitative Research in Psychology*, *11*(1), 25–41. https://doi.org/10.1080/14780887.2013.801543

Röder, N., Wiesche, M., & Schermann, M. (2014). A Situational Perspective on Workarounds in IT-Enabled Business Processes: A Multiple Case Study. *European Conference on Information Systems*.

Šedivcová, L., & Potančok, M. (2019). Shadow IT Management Concept for Public Sector. *International Conference on Research and Practical Issues of Enterprise Information Systems*, *13*, 65–73.

Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers &Amp; Security*, *45*, 274–283. https://doi.org/10.1016/j.cose.2014.06.007

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management*, *54*(8), 1023–1037. https://doi.org/10.1016/j.im.2017.02.007

Silic, M., Silic, D., & Oblakovic, G. (2016). Influence of Shadow IT on Innovation in Organizations. *Complex Systems Informatics and Modeling Quarterly*, *8*, 68–80. https://doi.org/10.7250/csimq.2016-8.06

SoftwareOne. (2023). *What is Shadow IT?* https://www.softwareone.com/bg-bg/solutions/software-lifecycle-management/shadow-it

Spierings, A., Kerr, D., & Houghton, L. (2017). Issues that support the creation of ICT workarounds: towards a theoretical understanding of feral information systems. *Information Systems Journal*, *27*(6), 775–794. https://doi.org/10.1111/isj.12123

Stewart, D. W., & Shamdasani, P. N. (2014). *Focus Groups: Theory and Practice*. SAGE Publications, Incorporated.

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, *11*(14), 2181. https://doi.org/10.3390/electronics11142181

Tambo, T., & Bækgaard, L. (2013). Dilemmas in Enterprise Architecture Research and Practice from a Perspective of Feral Information Systems. *Enterprise Distributed Object Computing*. https://doi.org/10.1109/edocw.2013.38

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42–57. https://doi.org/10.1016/j.cose.2014.05.003

Torii. (2022). *The State of SaaS at Work*. https://info.toriihq.com/the-state-of-saas-at-work-report

Walterbusch, M., Fietz, A., & Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. *Journal of Enterprise Information Management*, *30*(4), 644–665. https://doi.org/10.1108/jeim-07-2015-0066

Walters, R. (2013). Bringing IT out of the shadows. *Network Security*, *2013*(4), 5–11. https://doi.org/10.1016/s1353-4858(13)70049-7

Wieringa, R. (2014). Design Science Methodology for Information Systems and Software Engineering. *Springer eBooks*. https://doi.org/10.1007/978-3-662-43839-8

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. M. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45–55. https://doi.org/10.1057/ejis.2011.51

Yardley, L. (2000). Dilemmas in qualitative health research. *Psychology & Health*, *15*(2), 215–228. https://doi.org/10.1080/08870440008400302

Zimmermann, S., & Rentrop, C. (2014). On the Emergence of Shadow IT - a Transaction Cost-Based Approach. *European Conference on Information Systems*.

Zimmermann, S., Rentrop, C., & Felden, C. (2014). Managing Shadow IT Instances - A Method to Control Autonomous IT Solutions in the Business Departments. *Americas Conference on Information Systems*.

Zimmermann, S., Rentrop, C., & Felden, C. (2017). A Multiple Case Study on the Nature and Management of Shadow Information Technology. *Journal of Information Systems*, *31*(1), 79–101. https://doi.org/10.2308/isys-51579

Appendix

Appendix A: Conducting literature review

To identify and guarantee the quality and trustworthiness of the collected literature. This section discusses the sources, literature criteria, search terms, selection, and analysis of the literature.

The literature review starts with the selection of databases. In that regard, the databases Google Search, Google Scholar, Scopus and WorldCat are used. Scopus and WorldCat are utilized because they have an extensive academic database and great coverage of IS related topics (e.g., academic journals, articles, and e-books). Google Search and Google Scholar are used to search for "gray" literature (e.g., reports blogs and whitepapers). To search for suitable academic literature that aims to support the research, several inclusion and exclusion criteria are set to select relevant literature. Table 11 illustrates the inclusion and exclusion criteria used to select relevant literature.

Table 11. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
• Academic journal papers that discuss SIT. • Academic journal papers that discuss management or security frameworks, such as COBIT, ITIL, ISO/IEC 27000 series and NIST SP 800 standard series. • Academic journal papers that are published in leading peer-reviewed journals. Peer-review processes help ensure high quality. • Academic journal papers that are published in English.	• Academic journal papers that are not related to the research questions of this study, such as technical implementations of deterring SIT. • Inaccessible literature. • Academic journal papers that are not published in English.

Table 12 defines the search terms to find relevant literature. The base search terms are sometimes combined or replaced with other keywords indicated with "AND" or "OR".

Table 12. Search terms used during literature research.

Search term		Variations
"Shadow IT" OR "Workaround Systems" OR "Federal systems" OR "Rogue IT"	AND	"Definition" OR "Challenges" OR "Risks" OR "Benefits" OR "Causes" OR "Effects" OR "Characteristics" OR "Impact"
"Framework" OR "Security Framework" OR "Governance Framework"	AND	"COBIT" OR "ITIL" OR "ISO/IEC" OR "NIST"

After finding the databases, criteria, and search terms, the selection and analysis of the literature commences. The selection and analysis of the literature will be conducted and loosely adapted from the five-step literature review method of Wolfswinkel et al. (2013); this includes filtering out duplicates, refining the sample based on titles and abstracts, refining the sample based on full text, forward and backward citations and reiterate the process till no new articles are found. Figure 7. displays the above-mentioned selection process and the final selection of academic journals.

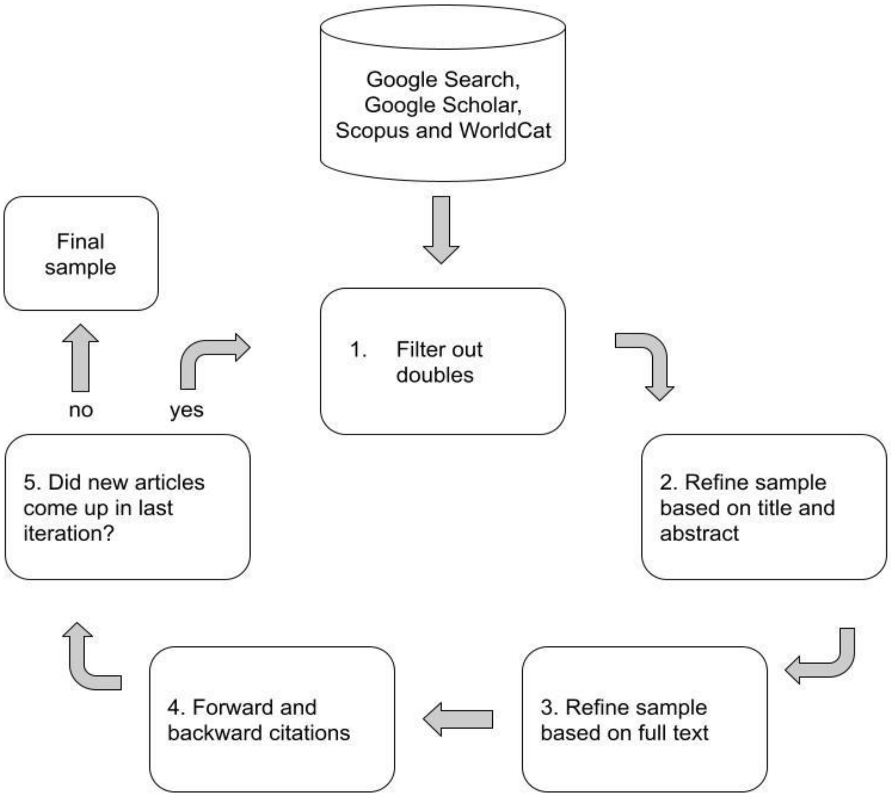

Google Search, Google Scholar, Scopus and WorldCat
1. Filter out doubles
2. Refine sample based on title and abstract
3. Refine sample based on full text
4. Forward and backward citations
5. Did new articles come up in last iteration?
no
yes
Final sample

Figure 8. The five-step literature review method by (Wolfswinkel et al., 2013)

Appendix B: Interview protocol

Phase	Protocol
Introduction	• **Thank the participant for his/her time.** • **Introduce myself and the research topic:** Hello, I am Kevin. I am currently a master Information Management student at Tilburg University. I am writing a thesis as a graduate student, and my research includes developing a risk management framework concerning shadow IT (SIT). The aim of this framework is to create a guideline for organizations to mitigate potential security incidents caused by SIT. • **Mention the duration, anonymity and recording of the interview:** The interview will take approximately 30 minutes to 1 hour. With your permission, I would like to record the interview so that I can transcribe it and thoroughly analyze and process the data. The interview data will be anonymized and will be treated as confidential. The recording of the meeting will be deleted after research completion. • **Ask if the participant has any questions.** • **Notify the participant that the recording will start.**
Background	1. Can you tell me about your role, specialization, and years of expertise in the field of risk management? 2. What is your experience with SIT and its impact on organizations?
General questions about SIT	3. Can you tell me about risks associated with SIT, both for individual users and for organizations as a whole? 4. Can you tell me about how organizations typically respond to instances of SIT? Are there any strategies or tools that are commonly used? 5. Which instances of SIT has the highest severity in organizational risk? (Cloud services, installed applications, self-made solutions, personal devices) 6. Can you tell me about key challenges that organizations face when trying to manage SIT?
Specific questions in SIT risk management	7. Can you tell me what role employees play in managing SIT, and what they can do to help prevent it? 8. Can you tell me what IT departments typically do to respond to SIT, and what steps they can take to better manage it? 9. Are there any existing frameworks or models for managing SIT that you are aware of, and if so, how effective do you think they are? 10. What features or capabilities would be important in SIT risk management framework?
Conclusion	11. Based on your experiences and expertise, what recommendations do you have for organizations looking to manage SIT better?

Appendix C: Thematic analysis

Theme	Code	Participant	Data sample
Determinants	Technical accessibility	S1	An example is the use of Google Translate because of its accessibility and performance.
		SM1	A practical example is to have awareness that a user is not allowed to use their personal OneDrive or Dropbox to share client files because of convenience.
		SE1	... we get emails that mention for example not to use Google Translate
			Samsung employees putting their whole source code into ChatGPT because initially they thought of it as a productivity tool and ease of use.
		P1	... unwanted behavior of IT services such especially cloud services like Dropbox that are easily accessible.
		SE3	Because most often employees seek out alternatives that are readily available
	IT user competence	S1	They go out on their own and search for better alternatives, because most often they are quite tech savvy.
		M1	Individuals are always trying to find efficient ways of working.
		SE2	I think that employees are getting smarter in conducting their way of working to save time and hassle whether it is with tools provided by their company or external tools.
	Poor business-IT alignment	M2	We might suspect that it's there, but you never really encounter it because the applications are more central from a business point of view.
		P1	That is probably one of the challenges for IT operations teams as they have limited resources to determine priorities to actually monitor SIT instances.
			To transform to such an environment, it requires up-to-date management network tools and that is quite hard to execute with traditional management tools.
		S1	... it is sometimes quite difficult to get a clear view of your overall infrastructure and to keep that accurate on a large scale. The reason can be that there is little alignment of management between the business and IT regarding control and decision-making.
		S2	I think that the business department is responsible and not the IT department. Because the business is responsible for the information of the assets.
		SM1	Usually, it is either the responsibility of the IT department or external service provider.
			Throughout the years, the responsibility has increasingly shifted towards the business because they are the end-users of the cloud service. In addition, the IT department is not even involved in the actual purchase or use of these services. I would say that IT departments would not be responsible for SIT management.
	Shortcomings of IT systems	M1	Individual users often look at an easier and time efficient manner and look for alternatives when companies can't provide it.

		P1	The individuals in the organization also just want to perform their work duties and while doing so face friction with existing available company tools.
		S1	They go out on their own and search for better alternatives
			The main issue you hear in those stories is that people are not content with the provided tools by their employer
		SE2	When a company provides tools that are very difficult to use then it is more likely for an employee to consider the use of SIT.
			... the main reason for the use of SIT is that a company does not provide the proper tools for employees' productivity.
	Misalignment of IT governance	M1	I also think that when an individual uses a cloud solution that is not allowed by the company and the cloud solution is based in the US, then the US legislation is applicable to that environment. For instance, when the US is saying you can't utilize the applications for work that include countries such as Iran. Then you can't use that service because of that legislation. In essence, there is a geopolitical factor to consider.
			It is not always a risk if individuals are using SIT tools, it is more the case if its compliant with company policy
			I never heard that they are giving an individual specific fines because they used external tools that were not allowed. They're getting a slap on the fingers, but I never heard that they get a fine or other repercussions.
			However, in a lot of cases employees don't ask the IT department for permission to use certain applications
		M2	... most organizations will have some degree of reactionary response. However, they won't look for SIT in a lot of cases.
		P1	I do notice that many companies don't spend the resources and time to monitor unwanted behavior in terms of internet usage. It is even more difficult when it comes to unwanted IT devices.
			Because not all companies are scanning the whole internal network and if you scan the network then you mostly do it for detecting unpatched systems and systems that can have vulnerabilities because of misconfigurations.
			I do notice that many companies have an end-user policy describing that they should only use the IT and software that is being provided by the company. The tricky thing is that although it's mostly implicitly mentioned, and sometimes explicitly.
		S2	The pitfall for organizations is that they have a lot of cybersecurity measures, but don't have an idea of their total asset management. Then it becomes really hard whether those controls are justified.
		SE2	For employees the risks could be repercussions by management
			Companies don't know how to respond to SIT.

			When an organization still provides individuals with not good enough tools and prevents the use of SIT as a whole. The risk of preventing SIT is that employees will search for other SIT applications that take its place.
		SE3	Organizations do have security measures in place, but a lot of organizations do not put much consideration into SIT risks. The organizations don’t consider SIT as a high risk.
			The tricky part with SIT is that the software and the hardware that you use might not be compliant to the organizational rules or the organizational policies, the security settings, that kind of stuff.
		SM1	Some other organizations don't mind SIT that much or are not aware of it.
	Lack of awareness	M1	It’s more a lack of user awareness that they are creating a specific risk for the organization.
		M2	As long as the application works then everybody will believe it's part of the normal IT landscape.
			I think you don't always realize how much SIT is actually used such as if you put client information within WhatsApp to a colleague. That is already in breach of that rule.
			Nobody's going to tell you that there's going to be SIT because nobody calls it SIT.
		P1	When individuals start using web services it doesn't always feel like they use third-party software.
			Most employees in larger firms don’t have a clue who to speak to when they face certain issues.
		S1	I think the main risk on an individual level is the lack of awareness. They don't know what they are installing and getting into their organizations network
		SE2	Another reason is that employees are unaware that they are not compliant with organizational policies.
Positive effects	Productivity gain & innovation	S1	People only see the productivity of the tool and they don't consider the information risks for organizations.
		SM1	I don't think SIT as a whole should always be fully avoided. If you are allowed to only use authorized software by the organization, there are a lot of exceptions where this may slow down innovation or productivity as a whole. However, I think the major risks related to SIT should be reduced as much as possible.
			The user needs to have a certain freedom for productivity and innovation
	User satisfaction	SM1	For individuals, I think SIT is really convenient.
			For example, when I first started within the organization, I had to make a lot of screenshots and edits of documents. I got the recommendation from a colleague to use an alternative open-source software application. But strictly speaking, that's also considered as SIT, because it's not authorized by the organization. Usually, SIT is the result of the laziness of the user. It is not necessarily always bad.
Negative effects	Security risks	M1	... when employees are not compliant with the company policy it could lead to a data breach

			That would be intellectual property, which would reside outside of the organization.
		M2	Which in turn may result in loss of data due to faulty programmed software by the employee or even incorrect data, which is even worse because everybody believes the data is correct, but it isn't.
		P1	The organizations often lack control of management and face security issues.
			Usage of personal devices in organizations introduces data security issues as those devices are connected to the organizational network.
			The risk of using open-source software is the probability of its security and the risk of third parties having direct access to your computer.
		S1	The risk of SIT is that it can lead to a data breach
			It could have consequences for them as individuals with their own private information leaking
			It can have consequences for the organization because they are very dependent on its people handling the information. The confidentiality of the data is at risk, which through SIT can get outside of the organization quite easily.
		S2	Another risk is cyber risk and that can be viruses, malware, and ransomware and that is a bigger threat to an organization.
			The individual risk is that a person’s data due to SIT usage is published without consent or that an entity uploads personal data into the cloud without permission. The privacy risk needs to be considered and is linked to individuals, and these can be privacy compliance, and regulatory compliance.
			That would be a data leak where individuals or an organization processes data without consent.
		SE1	If you're working with confidential data that is cybersecurity related or incident related and to use applications outside of the company can be considered a risk.
		SE2	The most common risk would be the use of third-party file transfer tools which may not be managed by the business entity and therefore companies don't know where that data is processed or if it's secure.
			... introducing security threats to the organizations such as viruses, malware, other data breaches, and data leakages.
		SE3	The primary risk we encounter is the use of SIT that weakens network security in the organization.
			I think when you look at employees that they have a crucial role because in almost all cases a person can be linked to a data breach or incident.
	Integration risks & data inconsistency	M1	We focus on those processes and it's a hard topic for other risks to verify that the data is complete in which all the data processes are implemented in that specific system. Most of the time we are not aware that they are using a separate system for SIT where they're using specific tools, for instance for purchase orders.
		M2	I have had multiple situations where I have heard that certain departments would use a specific SaaS

			solution to plan something that went outside of the normal planning application. You would always hear that it would lead to data issues such as inaccuracies or that it did not contain the appropriate information.
			If that information is put in in a separate system that differs from the main IT applications, then during the auditing process incorrect statements may surface.
			... the data being entered in the SIT application can’t guarantee that it is also implemented in the central IT application appropriately.
		P1	The use of such services can harm the confidentiality, availability of services and the integrity of data if things go wrong.
		SE2	Another challenge is to address the employees to quit using SIT applications. In certain instances, a whole team has set up a whole work process that runs on SIT.
	Control loss	M2	... when considering the privacy risks that an organization would adopt because they don't know which agreements are made because external parties can follow different security policies.
			I think the main risk would be integration and lack of a complete overview as it can cause all types of different problems.
		P1	The most frequent issue is that when unmanaged services exist there are limited to no security controls in place. That is because those services are unknown to the organization.
			However, when source code is leaked to third parties that directly becomes the second important risk.
		S1	they need to contact the Dutch Data Protection Authority because of breach in compliance
		SE1	Because you don’t know where the information is stored and on which servers. You don't know how long it will be stored on servers of the cloud vendor.
			The most important risk for companies is to maintain confidentiality for clients. You have certain agreements with clients that you only use approved tools and to ensure that data is being kept securely and appropriately.
		SE2	Organization cannot meet security controls when individuals manage corporate data on SIT instances.
			An organization will lack an overview of its IT landscape and has limited ability to take protective measures.
			As you cannot manage the security settings such as password settings in contrast to company managed tools.
		SM1	A lot of organizations had the issue that they were not fully in control of the assets that they were having in their IT landscape, so some organizations had a really hard time and a lot of scanning and searching to find which IT assets do we have within our landscape
			I think for organizations it is a bit problematic if you do not know which IT assets you control, so you have a lot of SIT

	Synergy loss & inefficiency	M1	We have a system for keeping track of certain processes, but we don't know if other BUs use another system for creating purchase orders.
		M2	... you never know which data source is then the correct one. I don't care whether the business application or the SIT application that I look at, but I need to be looking at the one that provides the correct information.
			... they had to pay for a couple of months of the license before it stopped.
			... it's not always that SIT is bad. However, it becomes an issue when groups of people start using it, leading to inefficiency.
		P1	An example is that an organization uses a freeware service that acts as a collaboration tool, but within a short time a large proportion of employees begin using it. Then the organization must decide whether to remove or approve and purchase the software including considering it for additional security features within their work environment.
		S2	I learned that most of the organizations do not have a complete insight into all IT assets. In terms of software and hardware, they are unaware of what information runs through their organization.
		SE2	... organizations struggle to identify the entire SIT landscape
			They also acknowledge the risk that purchases can be made by employees' personal credit cards. That would be harder to detect on those financial invoices.
			The biggest obstacle for an organization is that they are unaware of SIT that is running or that they are aware, but they don't know how to identify the full landscape with what's going on.
		SM1	Another element relates to the financial aspect such as with shadow cloud applications, when keeping track of all the extra costs that relate to the use of this SIT?
Risk management	Current landscape	M1	I'm not aware of any specific frameworks that are designed for SIT that are available. I think it's embedded within the current available risk frameworks because it's quite a specialist topic, but it's more regarding software asset management. However, I think that the current embedded frameworks could be better in addressing SIT.
		M2	No, not really. I wouldn't know of any specific framework that deals with SIT specifically.
		P1	Most of the popular security frameworks don't follow NIST but follows Center for Internet Security (CIS) controls and it aligns with the list of SANS top 20.
			An organization becomes efficient when they need to move from implementing what they don't want to have towards enforcing to what they allow. Currently we adopt a stance that everything is allowed unless certain criteria tell otherwise, but we need to move towards an approach that nothing is secure. That is practically the way forward and that is also part of the Zero Trust architecture.

		S1	I don't know if there are specific tools to achieve that
			I don't know of any frameworks addressing SIT.
		S2	Yeah, I do know of the NIST framework, SIT is briefly outlined in one or two sentences. But I do not know of any specific SIT framework that explores it in detail.
		SE1	I don't know which tools an organization has in place to respond to such cases.
			No not really, I know about the risk management frameworks such as NIST, OWASP and ISO but I don't think they really have the details that can address SIT.
		SE2	I'm not aware of any existing frameworks specifically designed for SIT.
			The governance organization that I talked about earlier does implement the Baseline Informatiebeveliging Overheid (BIO) to implement the cybersecurity measures. It is based on the ISO 27001 and 27002 standard, and the BIO also addresses SIT within that framework.
			I believe that the BIO that follows ISO 27001 only states that when SIT is active within the organization that you have to identify it and fix it. It only states that and it does not go deeper than that and merely acts as a guideline and does not provide enough guidance to the full scope.
		SE3	Most often it is the case that you can see a lot of gaps in their control framework and risk framework in terms of SIT.
			I do not know if there's any framework specifically designed for SIT. However, I think that the NIST directives partly explain the risks of SIT.
		SM1	I'm not aware of any specific framework related to SIT. I can imagine that there are some frameworks, maybe the NIST cybersecurity framework to some extent.
			Frameworks such as NIST and ISO have controls related to security monitoring. But often that's being interpreted as identification of unauthorized access.
	Identify	M1	Asset management is important. I think most companies have an overview of devices within their IT environments. The framework would pinpoint hardware and software that an organization has in their inventory.
		M2	I think you should be aware you should look for signals
		P1	The first rule to follow is to know your hardware and the second one is to know your software. If you don't know both assets, then you can't protect what you don't know. Implicitly, protection against SIT is to follow rule number one and two ...
		S1	I think the main thing is first getting an inventory of what data has been used.
			Another part of IT is asset management, like actually knowing what hardware is being used within the organization, especially with aspects like Bring Your Own Device
		S2	I recommend controlling the organizational information flows. Because it is very hard for an

			organization to determine the right cybersecurity or privacy measures when they have no control of their information flows.
			An organization should start with a list of an overview of all their information assets.
			The first thing to consider is to identify all the information flows and that is also missing in a lot of information security policies or frameworks.
		SE1	I think it's important to make an inventory to know what kind of applications are used.
		SE2	The most important criteria within that framework should be to identify all SIT within your organization, so how do you get the big picture and total landscape.
		SM1	... organizations should prioritize detecting and mitigate unwanted applications or systems in their network
	Identify - network	M2	It's not in our CMDB. Why is it or not, CMDB?
		P1	An organization should scan their assets so they can compare it with their CMDB.
		S2	Asset discovery tooling is also used to identify all the hardware and software in an organization. Microsoft Defender can be used as a discovery and monitoring tool.
		SM1	It can be software and hardware with an assigned asset owner. Who's responsible for maintaining that asset or the responsibility to do so. You also want to have what is called the CMDB, a configuration management database. That's sort of a large database, in which you can enter all your assets and relevant data
			... identification of SIT would be to use software tooling to scan all the assets on the network and compare that to the CMDB that is in place. Any difference in terms of unaware assets within your IT landscape are shown and detected
	Identify - ticket	P1	From an employee's perspective they should ask the IT department for better services and if it is not addressed, they will use other tools instead.
		S2	When employees have questions, it is important to address to whom they can submit a specific request for the use of unauthorized SIT.
		SE3	Ideally you would have somebody reporting the SIT instance or that it came from network monitoring tools. A ticket should be created of the security incident so that it can be tracked until the risk has been resolved
			Lastly, we would want to have controls like how you follow it up and often that control is in the form of a security incident procedure in where a ticket is created when it has been detected and followed up on until the problem has been resolved.
	Evaluate	M1	A second action after the identification process of which applications an organization has in their environment is to mitigate the risk.
		M2	You need to have risk evaluation. To determine accepted risk and the degree of trust in people that

			would normally be a kind of risk evaluation control to take.
		SE2	When risks are identified they should evaluate and take the corresponding action.
			It comes back to determine the risk for the organization and how does SIT increases or decreases that risk. The impact of SIT on the overall organizational risk should be determined to gauge the risk appetite.
			In addition, you should address the ways to identify the different types of SIT.
		SM1	We also need to know which specific assets are under their control or within their environment.
	Evaluate - policies	M1	Organizations should determine their own security policy to determine which controls are needed to secure their environment for employees to comply. If SIT applications are compliant with the GDPR but clashes with the company policy, then it should not be used.
		M2	It's ongoing and the application needs to be scanned and determined and evaluate whether it's in compliance with the policies.
		SM1	to what extent do we need to control security because not having control of SIT at all a too big of a risk.
	Evaluate - risk type cloud services	S1	Cloud apps would be the most severe because the thing with cloud is you don't know where in the world the information is stored. In contrast, laptops or other hardware within the organization are more manageable for an IT department.
		S2	I would consider cloud services as one of the biggest risks. Because it's a control problem in terms of data privacy, because it is hard to determine who is the owner of the data and who should take the necessary measures. When the data resides in the cloud it is no longer within one organization’s control regarding what is happening to the data. The organization must trust the cloud service provider that they do not share the data with other third parties.
		SE1	I think cloud services are one of the highest, because people can store a lot of information.
		SM1	If you do use a cloud service such as Dropbox for example, then the information is leaving the company device and towards the cloud service provider. Then you have no more control over where this data is going and who has access to it. I would say that cloud services are one of the major risks out of these four.
	Evaluate - installed applications	M2	Installing a certain application in that sense comes from a software supplier. There's a lower chance of software vulnerabilities as it should work as intended. Because the company has all the incentives to make sure the application does.
		P1	I think installing software can be considered as the highest risk. The risk doesn't only imply that you can leak data to the external environment, but it can also be used by third parties to break into your network.

		S2	In terms of installed applications, that is also a severe risk because of the possibility of introducing vulnerabilities in the organizational network.
		M1	A close second would be the installation of applications, that would be typically the same. It is hard to detect which applications your employees are installing, which connections are made from that application. Through the use of such applications, you could create unwanted VPNs that can create links to specific environments which the organization is unaware of. There is also the risk of unawareness in the specific scripting within the downloaded application that can create and execute all kinds of commands which can affect your device and company data.
		SE3	The most security controls needed to prevent security incidents would be downloaded applications, because security needs to be ensured for software that is used for work purposes.
	Evaluate - personal devices	M1	I believe that the use of personal devices can be deemed as one of the highest risks, because the IT department determines by default which applications are installed on company devices. The use of organizational data on a personal device is a total black box. If they're using the laptop at home, where they can use file transfer applications such as Google Drive, Dropbox, etc. then it is not routed to the company network. Because also when working from home you are not connected to the organizational network where a company could block specific websites.
		M2	I would say the using personal devices. I think it has a very high risk because you're taking data out of a secure organizational ecosystem. We all know the horror stories of people that don't update their phones and that are completely vulnerable. In addition, that on a personal device no restrictions are taken into place in terms of data security.
		SM1	The second one would be personal devices because sometimes if people get lazy, they use their personal device for work related stuff.
	Evaluate - self-made solutions	M2	Basically, I think another one that might be relevant is self-made solutions, because even if that ultimately serves its purpose. It introduces a whole problem of reliance on a piece of software that you're not having a maintenance contract for. Nobody feels that they have an obligation to maintain it and work as intended.
			You can’t say the same for something for an Excel macro developed by an employee that barely understands how something works and how the scripting works. Which in turn may result in loss of data due to faulty programmed software by the employee or even incorrect data, which is even worse because everybody believes the data is correct, but it isn't.

			The same goes for developing a macro that you use yourself, but it's completely different if I start distributing that to my colleagues.
		P1	Regarding self-made software, it is not the biggest issue if it is making your own programs that are used for productivity.
	Evaluate - risk types	P1	The highest risk is when malicious software enters the premises of the internal network. I would not differentiate between the other three types as it depends on the way you use each instance.
		SE2	I think every type of instance needs to have different measures in place and require a different type of management.
			It really depends on the risk management of the organization in what is considered a larger threat than the other.
		SE3	I think that all four can be seen as a severe risk for organizations.
	Analyze	P1	A company first needs to determine the existing friction within the IT landscape and determine the reason why people use SIT.
			The organization should determine to not only switch off a certain SIT instance but improve their existing tools to address the overall issue.
		S2	Overall, it is important that organizations identify the needs of employees to minimize SIT.
		SE1	I don't think you want to block everything immediately because that makes it difficult for employees. I think you should have a look at the IT you provide for your employees and determine what is reasonable to use which kind of SIT or look for suitable alternatives.
		SE2	The core collaboration between the company and the employee is that the company needs to provide good enough, easy to use and secure tools for employees to perform their work.
			When an employee does not process client or organizational data then they can make use of SIT.
		SM1	There's a bit of a tradeoff made between the essential high-risk applications an organization wants to reduce and the lesser SIT risks that are acceptable. I think that the challenge is striking a balance in determining the risks and to what extent do you allow it.
		SE1	I think that's important and to make an analysis on it
		S2	SIT is created due to a discrepancy of the desired work efficiency and as a company you can negate that if you listen to your employees and bring the necessary solutions.
		M1	I think there should also be an analysis when an application is operating in a gray area and investigate if the SIT instance is compliant with security policies
			They should also look at the number of users and for which purposes the SIT tool is used.
		SE3	The organization should also analyze the usage patterns and activity levels of the SIT instances to get a clear judgment.

	Respond	SE1	You can block and then monitor the kind of applications that are deemed too much of a risk.
		SE2	You can deny people using it or you can say that the in-house tools are not that good and consider for allowing the SIT tool.
			The next steps should be that you take a risk-based approach and determine which SIT is problematic and per SIT instance determine to accept or block it.
			The main takeaway is to determine and address which risks are the most severe to your organization and to follow up from that.
			The risk assessment should be to consider whether to accept or block certain SIT cases.
		SE3	An organization needs to consider which applications or devices to approve or not to approve to strengthen their network security.
			The best approach to managing a security incident is to have a procedure in place. This includes detection and response and that is always based on the organization’s procedures.
		SM1	That is regarding how do you perform vulnerability scanning on certain assets that you may not be aware of.
		S2	... that is also a severe risk because of the possibility of introducing vulnerabilities in the organizational network.
		P1	The organization needs to ensure to maintain their asset inventory and then address unauthorized assets.
	Monitor	M1	The devices are scanned and monitored for unwanted software on all devices.
			You could also consider that the use of unwanted hardware and software is monitored and that is based on other risk factors. I think in general way there should be control within a framework that is to frequently monitor which applications are used within the environment.
		P1	To monitor improper behavior a possible option could be to determine a list of unwanted services and enforce it with a firewall that blocks such services or sets alerts.
			Organizations can proactively monitor and block internet traffic in advance. You can ensure and approve only authenticated devices and software within the company network.
			Organizations need to have continuous security controls to monitor and manage their assets.
		S1	It's very important to keep the business resources separated on personal devices. For instance, you can have virtualization on that device to keep separate company applications and private applications. It's knowing exactly what's installed on devices, what devices are in the network, maybe even what they are authorized to do within the network.
		S2	I would say monitoring, logging, and evaluating.
			… make use of asset discovery and monitoring tools
		SE2	Ideally, a company needs to monitor the outgoing and ingoing internet traffic.

		SE3	The main challenge is the detection capability because automated monitoring and manual monitoring of such instances is hard to implement.
			Moreover, an organization should have detective controls. For instance, network monitoring, to look out for any irregular activity and act ahead of time.
	Prevent - policies	M1	Other companies in industries maintain companywide policies that users can't install any application. It also depends on the individual and job title which needs to use the SIT environment.
			University researchers are allowed to use SIT, but for students and employees that reside on the business side of the university, they aren't allowed to use it and it is being monitored.
			You would also have to determine the risk of SIT and then list a policy that which applications and devices are excluded from your environment.
		M2	You really need to be sure that agreements with all of these suppliers are in place, because if there's a leak at one of the suppliers and it contains patient information. Then you're still liable.
			... take disciplinary action against the employees that had implemented the SIT instances.
			I think it comes down to how you manage individual responsibility
			Depending on the circumstances, then you should provide more or less security measures for the use of such tools.
			... you need to establish a balance between what is allowed and not allowed and that is unique for each organization and that might be specific for a department, BU or sub-section.
			An organization should have the correct level of trust in their employees. It can be quite tricky to determine that level. It depends whether you're giving them the tools to do their work.
			... think that's also always in the information security policy that we need to adhere to and follow. The organization needs to share which information is not allowed to be put in cloud services.
			You can have preventative controls where you don't allow people to install something, or that they are allowed to have.
			I certainly think that it differs by industry, so most healthcare institutions will completely lock down their computers because most of the healthcare professionals only need one or two applications to do their work.
			If policies are breached then you can fire them or you can act against them, which in turn also prevents people from doing it because they know they will be held liable.
		P1	Organizations should at least have a policy in terms of what is allowed in terms of hardware and software. Otherwise, an organization cannot identify the unauthorized tools
		S2	I think that the business has the responsibility in determining SIT guidelines in the code of conduct.

			Repercussions can be given to individuals or organizations in the form of penalties.
			In addition, organizations are obliged to comply with laws and regulations, and it differs per industry as medical industries have more measures in place because they deal with personal health records.
			In addition, the organization needs to make sure that SIT is included in their code of conduct.
			To ensure that SIT is part of the code of conduct and that employees know which behavior can lead to specific sanctions.
			The compliance policy should make it clear to which hardware and software is allowed to be used.
		SE3	It is easier to implement security policies that you can share among employees regarding which software and hardware they cannot use.
			Organizations can adopt preventative control such as policy and procedures that are designed to prevent SIT usage.
		SM1	Maybe a control related to governance and policy that discusses to what extent is SIT allowed.
			... the security policy details to what extent a certain use of open-source software is allowed. You need to determine a certain level of flexibility and use of IT assets. In addition, a certain level of responsibility to the user is also assigned.
	Prevent - filtering	M1	Universities have a whitelist of applications which can be used for regular employees and maintain a blacklist of blocked web applications and installed applications
			If the scanned applications are listed on their own whitelist, it is deemed acceptable and if not, the application is deleted.
		M2	You have to provide a reason why you're installing it. I can guarantee you that IT in the background is running a scan on our laptops and if they find any software that is not in the list of approved software for which the license is needed, you will get an e-mail and you will get a call.
			That with respect to cloud services with examples like ChatGPT or Dropbox a company should block that on a network level.
		P1	At the moment most filtering is based on unwanted network traffic. If you are going to filter on what is allowed instead of what is not allowed, it means that you can issue a better filter in company data traffic.
			The Microsoft Intune application can also manage authorized applications on these devices. Those applications can limit the possibilities that you can do on those devices.
			And in terms of cloud services, you can have filtering options on your firewall that blocks certain URL's from visiting, which is URL filtering. You can set it up with a personal firewall, external firewalls, or the firewall in Azure.
			Palo Alto has subscription software that can analyze, and filter specific URLs and it can set up a profile of applications or tools that you allow and not allow.

			In addition, preventive controls can include URL blocking for unauthorized services, and you can have authentication of physical hardware.
		S2	Organizations can take preventive measures, such as policies in which they restrict certain services or devices with logging, monitoring, whitelisting, blacklisting, firewalls, and VPN’s.
			Preventive measures also need to be considered such as white listing, VPNs, and vulnerability scanning.
		SE2	Prevention measures should also be put in place so that such applications that are deemed too high of a risk, that users cannot download those tools.
		SM1	One example at a client Microsoft Intune is used and it is not really a SIT management tool. It is a tool to regulate which applications are authorized to be installed. It is a preventative approach to SIT.
			In practice it's mostly focused on trying to prevent SIT as a whole by blocking URLs, blocking firewall traffic, blocking certain applications from being installed and limiting the access rights that a user has on a device.
	Prevent - awareness and training	M1	I think creating awareness for the employees is the biggest challenge for a company.
			I think the employees should file a request to the IT department to say that their current work productivity is not efficient and if there are alternatives within the company that is to be used.
			Awareness is hard to teach to employees and the only thing you can do is to make it repetitive. To give and educate employees on a frequent basis interactive trainings, web learnings or something like that.
		M2	You can ask him to take responsibility for the actions he takes on the computer, but I also think it depends on what somebody should be able to do and the level of IT knowledge somebody has.
			The organization needs to trust employees in their knowledge that they can’t install a tool with an illegal license even though it would be more convenient.
			People should consider that there's also a price for using it because if they do use it then they have to explain why they processed certain client data within those applications. And that's a good thing as you need to be aware of the risks.
		P1	The users need to be very aware that they shouldn't use it.
			They need to ask the IT departments to ask for certain tools that they need. It should also address for employees how easy it is to resolve their problem.
		S1	First check with a manager and look for a tool within the organization that is available that can deal with the situation. Furthermore, if there is no such tool available within the organization. Ask your manager for something which could be reasonably used that isn't within the organization.
			Awareness and asset management are very important. Moreover, for an organization it would be preferable to look for the needs of your employees.
		S2	They have to comply with the organization’s code of conduct and penalties are included. An employee

			should be aware of the risks they are facing when they process sensitive information with external tools. Because it is their own responsibility when they upload the information.
			If they still want to use the tool, they should have a conversation with the IT department to make sure that they understand the desire to use the tool.
			The organization should give awareness workshops to make sure that employees know the risks of SIT. They should be easily approachable whenever employees have questions regarding using SIT instances.
			I would make sure that there's awareness among employees.
			It is recommended for organizations to commit to raising awareness among employees about the risk of SIT, for example by offering training, workshops, or simulations to employees.
		SE1	Of course, you need to educate your employees to let them know to what extent is the use of SIT possible
			I think you need to educate them and inform them about the risk and let them know in what way it can be used. You can’t prevent them from using it because I think blocking these instances doesn’t work as people will find a way to circumvent it
		SE3	In terms of creating security awareness is an important step if you want to reduce the risk of SIT, because if your employees do not follow the guidelines or the procedures that you implement, then the controls are not effective.
			There's a lot of research showing that new forms of training can be implemented to harden the employees and to create a more security aware organization. The training sessions can be simulation exercises in which different scenarios are played out and employees need to respond to that and will learn from it. Those simulations are more ingrained in employees’ memories than conventional training methods.
			I think it's a shared responsibility because when you look at security awareness. All BUs and all IT people need to be trained on these security issues. Everyone has a responsibility in terms of each control.
		SM1	I think that employees should have awareness of what exactly SIT is and what assets are allowed within the company policy.
			Creating awareness is an important thing, but an interesting element as well is that security awareness is very often not translated to actually secure behavior.
			... the organization needs to measure employee behavior, that employees actually display more secure behavior and otherwise adjust their approach if it is not deemed effective

Appendix D: Validation questions

Phase	Protocol
Introduction	• **Thank the participant for his/her time.** • **Introduce the process of the validation interview:** During this interview • **Mention the duration, anonymity and recording of the interview:** The interview will take approximately 30 minutes. With your permission, I would like to record the interview so that I can transcribe it and thoroughly analyze and process the data. The interview data will be anonymized and will be treated as confidential. The recording of the meeting will be deleted after research completion. • **Ask if the participant has any questions.** • **Notify the participant that the recording will start.**
1st round of validation questions regarding the conceptual framework	1. What is your general opinion of the developed framework? 2. What is your general opinion of the visualization of the developed framework? 3. What are your thoughts on the "Prevent" phase? 4. What are your thoughts on the "Identify" phase? 5. What are your thoughts on the "Evaluate" phase? 6. What are your thoughts on the "Analyze" phase? 7. What are your thoughts on the "Respond" phase? 8. What are your thoughts on the "Monitor" phase? 9. Do you find the developed framework complete, useful, and reliable? 10. Do you have any other comments regarding the developed framework?
2nd round of validation questions regarding the adjusted framework	1. What is your general opinion of the developed framework? 2. What is your general opinion of the visualization of the developed framework? 3. What are your thoughts on the "Prevent" phase? 4. What are your thoughts on the "Identify" phase? 5. What are your thoughts on the "Assess" phase? 6. What are your thoughts on the "Respond" phase? 7. Do you find the developed framework complete, useful, and reliable? 8. Do you have any other comments regarding the developed framework?