CHALMERS
UNIVERSITY OF TECHNOLOGY

TRAFIKVERKET
SWEDISH TRANSPORT ADMINISTRATION

Auditing an Internal Audit Function

Incorporating Risk- and Knowledge Management Practices to Achieve an Effective Internal Auditing

Master's thesis in Quality and Operations Management

OSCAR SIMONSSON
LOVISA SVANLING

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF INNOVATION AND R&D MANAGEMENT

CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2024
www.chalmers.se

Auditing an Internal Audit Function

Incorporating Risk- and Knowledge Management Practices to Achieve an Effective Internal Auditing

OSCAR SIMONSSON
LOVISA SVANLING

Department of Technology Management and Economics
Division of Innovation and R&D Management
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2024

Auditing an Internal Audit Function
Incorporating Risk- and Knowledge Management Practices to Achieve an Effective Internal Auditing
OSCAR SIMONSSON
LOVISA SVANLING

Department of Technology Management and Economics
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone + 46 (0)31-772 1000

Gothenburg, Sweden 2024

Auditing an Internal Audit Function
Incorporating Risk- and Knowledge Management Practices to Achieve an Effective Internal Auditing

OSCAR SIMONSSON
LOVISA SVANLING

Department of Technology Management and Economics
Chalmers University of Technology

SUMMARY

The purpose of this thesis is to explore improvements for conducting internal audits by incorporating risk- and knowledge management theories into the process. This thesis employed a qualitative research design focusing on internal auditing within the Swedish Transport Administration, a public organization. Using a case study method, the research included interviews, observation, and documentation to collect data. The aim of the case study was to explore how current practices of internal auditing can be improved by risk- and knowledge management practices. Findings show that the internal auditing within the Swedish Transport Administration has a well-established documentation of processes, outlining a structured approach describing *what* to achieve. However, in analyzing the results, it is evident that certain activities lack clear instructions on *how* to perform these activities, such as the supplementary risk analysis. In conclusion, this research found that while the internal audit process is well-documented, some activities lack standardized procedures, leading to individual ways of performing these activities. Implementing the Plan-Do-Study-Act cycle to the audit process and adopting knowledge management practices can establish common ways of working and facilitate continuous improvement. Furthermore, conducting risk assessments in the engagement planning through a proposed model can facilitate in defining scope and orientation for the audit engagement.

Keywords: Internal auditing, Knowledge management, Risk management, Continuous improvement, Case Study, Public Organization, Swedish Transport Administration.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

COSO	Committee of Sponsoring Organizations
IA	Internal Auditing
IIA	Institute of Internal Auditors
ISO	International Organization for Standardization
IPPF	International Professional Practices Framework
KM	Knowledge Management
PDSA	Plan-Do-Study-Act
RQ	Research question
SECI	Socialization, Externalization, Combination, Internalization
STA	Swedish Transport Administration

1. Introduction

Today, organizations operate in increasingly complex, dynamic, and competitive environments. Most changes in the business environment result in new or modified risks for organizations to consider (Betti & Sarens, 2020). It is essential for organizations to prevent risks to avoid negative consequences that may hinder organizational objectives from being achieved (Nichols, 2014), particularly as these risks are becoming significantly more complex (PwC, 2015). Furthermore, managing risks has gained increased importance among managers to ensure long-term profitability (Raiborn et al., 2017). In such circumstances, internal auditing can be utilized to govern and perform activities, such as risk management (Prawitt, 2003). According to the Institute of Internal Auditors (IIA) (2024), internal auditing is defined as:

> "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control , and governance processes."

Internal auditing is effective when it assists the organization in achieving its objectives (Lenz & Hahn, 2015). For this purpose, the internal audit function, which is the department conducting internal auditing activities within an organization, must identify and understand what risks may prevent the organization from fulfilling its objectives (Prawitt, 2003). Considering limited resources of the internal audit function, an annual audit plan is developed to be carried out in the upcoming year. The annual audit plan involves selecting and prioritizing potential audit engagements, which are auditable areas to be reviewed within the organization, and also to ensure that resources are allocated optimally (Wang et al., 2023). Additionally, internal auditors frequently state that their annual audit plan is based on risk. However, these are often made with an informal risk assessment and a vague understanding of the concept risk (Moeller, 2011).

In terms of effective internal auditing, Arwinge (2016) emphasizes the importance of a well-executed engagement planning, which is a process step to provide clear objectives and scope for the specific audit engagement. However, the literature highlights three common reasons for planning failures, including focusing the effort on less critical risks, or setting the scope either too extensive or too narrow (Arwinge, 2016). Furthermore, Anugraheni et al. (2022) also state that insufficient planning may lead to failure in achieving the objectives set for the audit.

Conducting audits can appear as a complex task with several parts to take into account (Nichols, 2014). The role of an internal auditor can be challenging having to possess a variety of skills within several areas and establish relationships spread over the organization according to Gasparotti and Gasparotti (2023). Furthermore, Mai and Nguyen (2022) state that internal auditing is a practice that is knowledge intensive.

Additionally, sharing knowledge between internal auditors may have a large impact on the quality and efficiency of an audit (Duh et al., 2020).

However, previous research suggests that studies focusing on knowledge management (KM) in connection to internal auditing are limited (Mai & Nguyen, 2022). Most of the literature is focused on internal audit quality and the related influencing factors, or how to evaluate internal auditing effectiveness (Kotb et al., 2020). Moreover, to our knowledge, most research of internal auditing relates to financial sectors, such as banking. Therefore, our research addresses how KM practices can be adopted in a different sector, dealing with other types of risks, to achieve higher levels of knowledge-sharing.

1.3 Aim

The purpose of this thesis is to explore improvement of internal auditing processes by incorporating risk- and KM theories. To fulfill the purpose, the following research questions (RQ) have been formulated:

RQ 1*: How does an internal audit function perform an audit in practice, and how is the audit process described in documentation?*

RQ 2: *How can an internal audit function strengthen risk management in engagement planning?*

RQ 3: *How can an internal audit function adopt knowledge management practices to improve audit engagements?*

In connection to RQ2, the research also aims to provide an applicable framework for risk assessment within engagement planning.

2. Theory

This chapter presents academic literature regarding quality management, auditing, risk management and KM. To address all RQs, quality management is explored to gain an overall understanding of the concept and how principles such as continuous improvement may be applied to achieve a more effective internal audit process. Auditing is a part of quality management, which is presented to facilitate an understanding of its processes according to academic literature. In connection to RQ2, theory on risk management is examined, aiming to provide an understanding of risk in relation to internal auditing and also to be used as a basis for strengthening risk management within engagement planning. Lastly, the literature of knowledge management is reviewed to comprehend how managing and sharing knowledge can be utilized to improve internal audit processes, aligning with RQ3.

2.1 Quality Management

Quality can be viewed as conformance to specifications for many organizations, while for others it is a subjective concept (Kuei & Lu, 2013). According to Kuei et al. (2008), quality can be seen as an outcome of quality management, stressing the need to be committed and detail oriented. Quality management can be described as a holistic philosophy promoting continuous improvements and organizational change of all departments within an organization (Kim et al., 2012). Continuous improvement is a central theme of quality management (Gremyr et al., 2020), which according to Manos (2007) can be defined as “subtle and gradual improvements that are made over time”. According to Morrow (1997), continuous improvement facilitates gradual improvements of business processes and associated work methods, often applied at a unit or individual level. Moreover, according to Sanchez and Blanco (2014), continuous improvement is a cyclical, ongoing process, and not merely an act performed occasionally.

2.1.1 Continuous Improvement

Improvements have since long been at the core of quality management, and different approaches for improvements has been developed and applied in various context over time such as Plan-Do-Study-Act (PDSA), Deming cycle, and Define-Measure-Analyze-Improve-Control (Gyllenhammar & Hammersberg, 2023). Furthermore, Gyllenhammar and Hammersberg (2023) argue that quality management has previously had a focus on product-oriented improvements but has since then shifted into becoming more widespread and applied in different contexts. This is also emphasized by Moen and Norman (2006), stating that PDSA can be applied in any organization to improve processes, products, and services. Nichols (2014) found that the PDSA cycle can facilitate in developing an effective process of internal auditing. The PDSA cycle is an iterative and systematic process which includes the following four phases, shown in Figure 2.1.

Figure 2.1: Phases of the Plan-Do-Study-Act cycle (Gremyr et al., 2020).

Firstly, objectives and plans are established aimed at improving e.g., the process during the Plan phase. Secondly, the plan is put into action through the implementation of improvement activities in the Do phase. Thirdly, during the Study phase, reflection and learning from the work done in previous phases takes place. Furthermore, results are measured to see whether the plan worked, and whether objectives have been met. Lastly, in the Act phase, insights gained from the Study phase are used. Unsuccessful ideas are rejected, while others are developed and implemented into the upcoming PDSA cycle (Gremyr et al., 2020). According to Gremyr et al. (2020), organizations can improve and move toward better performance and quality through many iterations and consistent use of the PDSA cycle. An idea behind PDSA is to start small and then scale it up upon successful outcomes. Hence, unsuccessful changes can be discarded, and the cost of testing remains low, as it was applied on a smaller scale. As PDSA combines action with reflection, it becomes a learning-driven process (Gremyr et al., 2020).

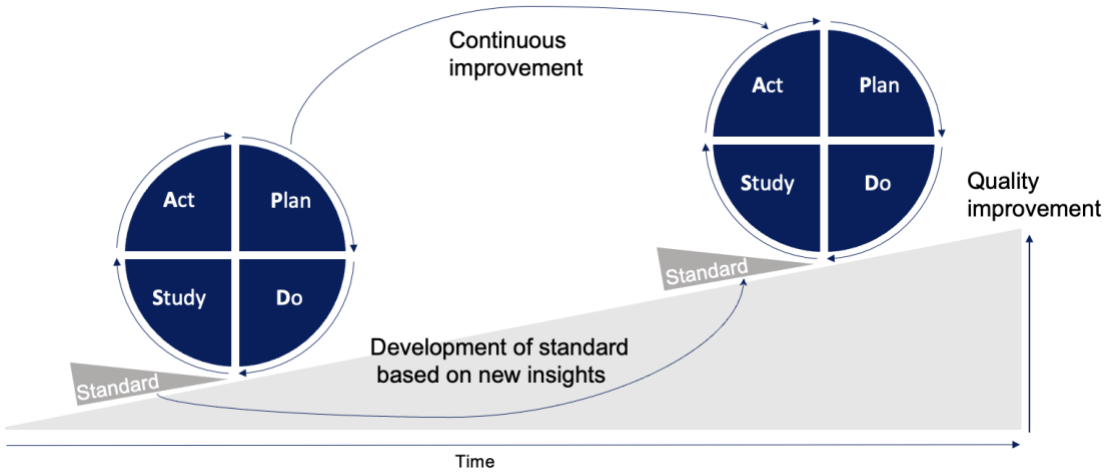

Figure 2.2: PDSA cycle and its link to continuous improvement (Gremyr et al., 2020).

It is critical to document improved work processes as new standard practices in the Act phase. This standardization is a means of ensuring continuous improvement over time (see Figure 2.2). However, an excessive focus on standardization may stifle innovation as it promotes exploitative actions rather than explorative ones (Gyllenhammar & Hammersberg, 2023). According to Ungan (2006) standardized processes should contain established documentation showing the relation between activities, employees, information and objectives in the specific work order.

Documentation should also be of a suitable level and easily understood. The employees working with mapping the process should decide the level of detail in documentation. Lack of detailed documentation allows employees to establish individual ways of working, which in turn can lead to a variation in the output (Ungan, 2006). Although processes are documented and standardized, employees sometimes choose not to adhere with the standardized process since they might find more efficient ways of performing the tasks, yielding better results (Nissinboim & Naveh, 2018).

2.1.2 Auditing

According to Hutchinson et al. (2024), audits are defined as a way of verifying that established procedures and associated results are being followed and that these procedures are effectively implemented and adequate to achieve the desired results. In addition, audits are covered and evaluated in the three areas of compliance, validity, and suitability to examine whether there are differences between expectations and reality (Hutchinson et al., 2024). Audits can be performed internally and externally, and an internal audit is performed by auditors employed by the company meanwhile external audits are outsourced and performed by external actors (Mehmeti, 2021). The primary objective of an external audit is focused on financial information meanwhile an internal auditor's objective is focused on the organization's overall operations and processes, identifying potential risks and improvements. Internal auditing has a wider scope covering areas such as compliance and risk management (Mehmeti, 2021).

While quality research has put a lot of emphasis on external auditing, the research made on internal auditing seems to be more limited (Samagaio & Felício, 2023). However, Samagaio and Felício (2023) further stresses the importance of internal auditing since it can be used as a tool for understand an organization from a realistic context, in order to make improvements on effectiveness and efficiency required for the organization to maintain its position. Lazarus et al. (2021) also argues that an optimal utilization of internal audit is required for organizational achievement of financial, operational and strategic objectives. In parallel with changes made in the business environment over previous decades, internal audit engagements have also evolved and continue to undergo changes constantly (Coetzee & Lubbe, 2014). Samagaio and Felício (2023) further elaborate on more recent events like COVID-19 and the financial crisis which also might have influenced the practices of internal auditing in terms of efficiency and quality.

In terms of internal auditing, different approaches for conducting internal audits exist, such as ISO 19011 and the International Professional Practices Framework (IPPF). ISO 19011 is a well-known standard providing guidance in auditing management systems, such as ISO 9001 and ISO 14001 (International Organization for Standardization, 2018a). Internal auditing according to the IPPF approach is described as an assisting role to the management of an organization, working towards continuous improvement by upholding effective and efficient control systems (Khairunnisa, 2020). On the contrary, Khairunnisa (2020) describes the internal auditing connected to the ISO approach as a similar concept. However, the focus when conducting internal audits lies in the requirements of the specific ISO-standard, aiming to determine whether an organization is following the set objectives to receive a

certification for that standard or not. Furthermore, the ISO 19011 framework provides guidance for both external and internal audits, according to Simon et al. (2014), meanwhile IPPF focuses on internal auditing solely.

2.1.3 The International Professional Practices Framework

The IIA has developed its IPPF to guide internal auditors in their profession and to ensure high-quality internal auditing at a global scale (The Institute of Internal Auditors, 2017). The framework is divided into two categories, Mandatory Guidance and Recommended Guidance, as shown in Figure 2.3. Mandatory guidance consists of a set of elements where conformance is required, including Core Principles, Definition, Code of Ethics, and Standards. Recommended guidance is optional and is designed to effectively assist in implementing the mandatory requirements.

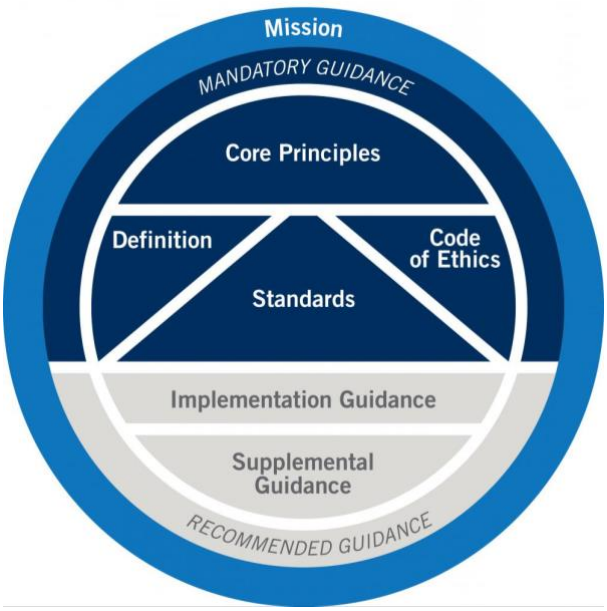

Figure 2.3: Elements of the International Professional Practices Framework, separated into mandatory guidance and recommended guidance (The Institute of Internal Auditors, 2017).

The core principles for the professional practice of internal auditing include integrity, competence, and due professional care. The practice also ensures objectivity, independence, and alignment with the organization's strategies, objectives, and risks, among other principles. Essentially, the core principles articulate effectiveness within the internal audit function. Moreover, all principles should be present and operating in order to achieve internal audit effectiveness. However, all organizations are not the same and the implementation of the core principles may vary, but failure of achieving any of the principles may lead to inefficiencies (The Institute of Internal Auditors, 2017). Furthermore, the purpose of the code of ethics is to promote a culture that is ethical in the conduct of internal audits. It states principles and expectations that govern the behavior of individuals and organizations in the conduct of internal audits. Additionally, the minimum requirements of conduct and behavioral expectations are described, rather than specific activities (The Institute of Internal Auditors, 2017). Lastly, the standards are principle-focused and provide internal auditors with a framework for performing and promoting the profession. The standards are mandatory requirements

including statements of basic requirements for the practice of the profession and evaluating the effectiveness of performance. It also includes interpretations that clarify terms or concepts within the standard (The Institute of Internal Auditors, 2017).

2.1.4 Engagement Planning

According to The Institute of Internal Auditors (2017), engagement planning is the process of developing and documenting a plan for each engagement. Furthermore, the engagement planning process is an activity performed by internal auditors. According to Rife (2006), the most important part of an audit is the planning for each engagement, which further elaborates by stating that inadequate planning e.g., can entail the need for adjustments of scope and objectives later in the audit process. Moreover, he argues that a carefully conducted audit engagement increases the possibility to achieve a successful audit, while fulfilling the aim and providing the organization with improvement areas (Rife, 2006). The definition of Engagement Planning according to The Institute of Internal Auditors (2017) is as follows:

> "Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement."

Effective planning of the engagement begins with gaining an understanding of the context and purpose. This includes understanding the internal audit plan and its development, the reasons why the engagement was included, and how the organization's mission, vision, and strategic objectives, among others, align with the process or area under review (The Institute of Internal Auditors, 2017).

To determine engagement objectives and scope, internal auditors gather information about the area or process to be audited. This may involve reviewing previous audit engagements, applicable policies and procedures, and interviewing relevant stakeholders to map the process or the area under review. Next, internal auditors need to prioritize risks to be evaluated further during the engagement. Thus, conducting a preliminary risk assessment, utilizing process maps, and brainstorming potential risk scenarios may aid in identifying risks relevant to the area or process to be audited (The Institute of Internal Auditors, 2017). After establishing the objectives and scope of the engagement, resources need to be allocated to achieve the objectives. Allocation of resources entails the quantity, and mix of knowledge, skills, and other competencies needed to accomplish the engagement (The Institute of Internal Auditors, 2017).

2.2 Risk Management

According to Hopkin (2012) risk management can be described as a number of activities performed to control organizational risks, aiming to protect the company. The risk management process can be divided into three steps: risk assessment, risk mitigation plan and risk management plan (Szabo, 2012). During an organization's development, the exposure of risks will appear (Krstić & Dordević, 2012). The general view of risks tends to focus on the potential negative consequences which may arise

due to risks, although it may also include potential positive consequences in the form of e.g., opportunities (Krstić & Dordević, 2012). Traditionally, risk management has focused on risk avoidance, however it prevented organizational development since opportunities were missed out (Krstić & Dordević, 2012).

According to Szabo (2012), risk management aims at managing an organization's operational and strategic risks which are essentially different from each other. The strategic risks can interfere with an organization's ability to achieve its objectives connected to the vision or strategy, while the operational risks might affect the performance negatively on the daily operations within an organization (Szabo, 2012). Hopkin (2017) introduces four types of risks, namely compliance risks, hazard risks, control risks, and opportunity risks. Compliance risks target risks linked to compliance of laws, rules, and procedures in which organizations often strive to minimize these risks. Hazard risks can be described as risks connected to a negative outcome, and organizations often mitigate these risks to an acceptable level. Control risks are associated with an uncertainty of an outcome, e.g., expected results versus the actual outcome of a project, and the organization strives to manage this type of risk since the outcome can be both negative and positive. Lastly, the opportunity risks where the organization sees the risk as an opportunity to attain a positive return.

All identified risks have an uncontrolled level which compares to the level before preventative actions have been assigned to minimize the risk value (Hopkin, 2017). Evaluating the risks using likelihood and impact are commonly used models to determine the risk level. Furthermore, Hopkin (2017) states that there are divided opinions when to perform risk assessment and whether it should be performed with consideration to existing control activities at a residual level or looking at the risk independent from existing control activities at an inherent level. However, the intention of it is equivalent and aims to understand the risk level combined with identification of already added controls (Hopkin, 2017). Implementing controls will reduce the risk level and can be associated with the name residual risk (Hopkin, 2017). According to Coetzee and Lubbe (2014), internal auditors can benefit from having knowledge about the movement between inherent and residual level of the risks in the beginning of planning for an audit engagement and associated procedures. Moreover, Szabo (2012) adds to this by stating that risks should be assessed in two steps. Firstly, inherent risks at strategic level, and secondly, residual risks at an operational level. Furthermore, a prioritization of the residual risks should be done, based on the knowledge of these existing control activities. There are several frameworks for managing risks in literature. Fox (2018) states that the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) enterprise risk management (ERM) and ISO 31000 are the two most widely used frameworks in risk management. Presenting these two frameworks will depict similarities and differences within different approaches of risk management to develop a general understanding of risk management.

2.2.1 Committee of Sponsoring Organizations of the Treadway Commission's Enterprise Risk Management

COSO was founded in 1985 by five accountancy and auditing organizations operating globally (COSO, 2023). In 2017, COSO released the latest version of the integrated framework ERM, which is a risk management framework aiming to facilitate risk identification, risk assessment and accomplishment of objectives (COSO, 2017). The framework is merging risk with strategy and performance to bring the perspective of risk through the entire organization (COSO, 2017). The framework consists of a number of principles, separated into five interrelated areas:

1. *Governance and Culture* - An organization's governance sets the direction for risk management, establishing and distributing responsibilities within the risk area. Culture reflects the organizational view of the ethical perspective, the common perception and comprehension of risk and established behaviors.
2. *Strategy and Objective setting* - Business objectives and strategy within an organization aligns with the risk management in the overall strategic planning. Setting a strategy for the organization will include the establishment of a level for risk tolerance and the objective-setting becomes a practical basis for identification, assessment and response to risks. The organizational strategy will therefore set a direction and level for the risk tolerance to achieve the strategic objectives.
3. *Performance* - The risks standing in the way of achieving an organization's strategy and business objectives may have an impact on performance. Therefore, it becomes important to identify and assess these risks and announce them to stakeholders. A risk prioritizing is done taking severity and risk appetite into account, followed by risk responses which are compiled in a portfolio.
4. *Review and Revision* - Examining an entity´s performance can facilitate an organization's ability to determine how the risk management works gradually, considering changes in the business environment and adjust accordingly.
5. *Information, Communication and Reporting* - Internal and external vital information from the entire organization should be shared and obtained continuously (COSO, 2017).

To support these areas there are twenty related principles aiming to facilitate organizations in managing things like control to surveillance. The principles are broken down into concrete practices with adaptation to a variety of organizations considering e.g. size and sector. The principles entail an understanding and ambition for the organization to consider risks linked to overall strategy and business objectives (COSO, 2017).

2.2.2 ISO 31000

ISO 31000 is an international standard developed and published by the International Organization for Standardization (ISO) which is a recognized body worldwide. The purpose of ISO 31000 is to provide generic principles and guidelines of establishing a risk management framework that is applicable to any organization regardless of its

size, industry, and type (International Organization for Standardization, 2018b). The principles of ISO 31000 highlight the importance of integrating risk management into all aspects of activities and decision-making processes within an organization. Furthermore, the principles also include an extensive and systematic method to risk identification and assessment, as well as continuous improvement and adaptation of risk management practices (International Organization for Standardization, 2018b).

The ISO 31000 framework for managing risk is structured around a process consisting of: establishing the context, risk assessment, risk treatment, and monitoring and reviewing (International Organization for Standardization, 2018b). The main output of establishing the context of risk management is defining the “risk criteria”, which is used to evaluate the significance of risk. Risk assessment includes identifying, analysis, and evaluation of risks to determine their potential impact and likelihood. Risk treatment involves selecting the appropriate controls, which are measures to modify risks. Lastly, monitoring and reviewing is essential to the process, assuring that controls are effective, lessons are learned, among others. In conclusion, the ISO 31000 risk management framework is comprehensive and flexible which can be adapted to any organization. The principles of managing risks and the risk management process enable a robust risk management strategy, which makes it attractive for organizations.

2.2.3 Risk-Based Internal Auditing

Emerging internal auditing with risk management is known as risk-based internal auditing which Coetzee and Lubbe (2014) explains as the internal auditor’s engagement in the risk management within an organization. Coetzee and Lubbe (2014) mention that a common perception of risk-based internal audit is the connection with organizational risks linked to the annual audit plan. However, Coetzee and Lubbe (2014) underline the ability to devote a risk-based approach within each audit engagements as well, using equivalent methods for risk management. This is also emphasized by Allegrini and D´Onza (2003) who claims that there are two levels for utilizing risk assessment into internal audit planning, one of them being in the annual audit plan (macro risk assessment) and the other one in planning for the specific audit engagement (micro risk assessment).

Coetzee and Lubbe (2014) mentions five steps to apply when performing internal audit engagements with a risk-based approach:

1. Setting objectives for the audit engagement that aligns with the objectives for the audited part of the organization.
2. Identification of strategic and operational activities within the engagement and also risks which may prevent the objectives of being reached.
3. Risk assessment including an evaluation of the parameter’s likelihood and impact.
4. Management should establish risk responses for the organization to implement, aiming to mitigate the risks.
5. Connected to the risk response, a set of control activities should be determined.

However, Coetzee and Lubbe (2014) also identified weaknesses in the performance of risk-based internal audits. The risk analysis and mitigation are seldom implemented in the audit engagement but instead the risk assessment consists of identification for controls, thus the control driven approach is often applied instead of the risk driven (Coetzee & Lubbe, 2014). Moreover, instead of relying on the formal risk assessment, already produced by the risk department, internal auditors usually carry out a separate risk assessment in the specific audit engagement (Coetzee & Lubbe, 2014). Furthermore, using the result of the formal risk assessment reduces the risk of doing the same work twice. However, this assumes that the organization is risk-mature and that internal auditors can rely on the risk assessment produced by the risk department. This can be assured by auditing the risk management process (Coetzee & Lubbe, 2014).

2.2.4 Risk assessment

Ramamoorti et al. (1999), describe the risk assessment process as a systematic approach for professionally reviewing risks and their associated factors, determining their significance and identifying the potential negative outcome for the risks. The risk assessment includes connecting the risks with control activities (Ramamoorti et al., 1999). Moreover, Pungas (2003) emphasizes the importance for internal auditors to conduct risk assessment, since it aids in achieving the objective of an audit, which is to predict potential risks within an internal control system and manage the risks economically and effectively.

Pungas (2003) describes the strategic audit plan as a way to structure the annual audits and to emphasize the prioritized risks that emerged from the risk assessment. However, Pungas (2003) further elaborate by pointing out the importance of considering other aspects, such as each business unit´s own initiative of activity plan, information compiled from former audits, and what internal auditors find appropriate and necessary to audit. Since the core of internal audit lies in managing risks and assessing controls, Pungas (2003) states that conducting risk assessment becomes an essential part when performing internal audits. Moreover, risk assessment becomes a foundation for determining priorities for the internal audit, which in turn affects the level of effectiveness and value for the audit engagements.

As mentioned before, Allegrini and D´Onza (2003) are highlighting the risk assessment in both macro and micro level when applying a risk-based approach of internal auditing. The risk assessment process defined by McNamee (1996) can be described in three steps including identification of risks, measurement of risks and prioritization of risks, mentioned by Ramamoorti et al. (1999). Furthermore, McNamee (1996) argues that the macro risk assessment should consider risks connected to the organization from a broad perspective e.g., objectives and processes, and on the contrary, micro risk assessment should refer to the audit program and what areas to be reviewed, orientation and scope (Ramamoorti et al., 1999).

2.3 Knowledge Management

KM involves managing and organizing all knowledge that encompasses an organization, or business environment. KM is focused on defining, developing and adjusting the knowledge base of an organization and acts as a vehicle for absorbing knowledge (Cordeiro et al., 2024). Having the right knowledge and the ability to transform knowledge for new value creation is considered to provide a competitive advantage. As a result, the interest of KM has drastically increased, and attention has been directed towards developing and maintaining organizational knowledge (Hock-Doepgen et al., 2021). KM is dependent on individuals sharing their knowledge, thus, it is important that organizations encourage a culture of knowledge sharing (Easa, 2012).

Knowledge occurs in many forms, such as competence and capabilities of employees, patents and licenses (North & Kumta, 2018). An internal auditor exhibits a broad base of knowledge, involving an understanding of professional standards, legal and regulatory requirements, as well technical expertise, knowledge of relevant industries, practical experience, and the ability to make professional judgement (Nguyen & Kohda, 2017). According to Nonaka & Takeuchi (1995), knowledge exists on many different levels, i.e., individual, group, organization, and inter-organizational. Sharing and managing knowledge within an audit firm could be a way to boost the audit quality. Auditors can share knowledge among each other in two ways: tacit and explicit. Tacit knowledge is often described as “know-how” and is embodied within an auditor’s mind or experiences and is hard to express or write down in a tangible form (Albawwat, 2022). In contrast, explicit knowledge is systematic and methodic and exists in an articulated form (North & Kumta, 2018). Such articulated forms include written documents, e.g., reports, which are easily shared among auditors. Sharing tacit knowledge among auditors requires more time and effort, which makes the process more difficult than sharing explicit knowledge (Albawwat, 2022). Notably, only a small fraction of knowledge is expressed explicitly in an organization, and knowledge becomes valuable for an organization in its explicit form (North & Kumta, 2018). However, there are limitations in converting tacit into explicit knowledge. For example, the ability to balance a bike while riding is a form of tacit knowledge that may not be fully articulated in its explicit form and thus remains tacit (Easa, 2012).

A common concept within KM is the SECI (socialization, externalization, combination, and internalization) model, developed by Nonaka and Takeuchi (1995) which include four ways of developing and transforming knowledge, tacit to explicit and vice-versa (see Figure 2.4). Nonaka and Takeuchi (1995) also argue that knowledge is developed by individuals initially but can be transformed to organizational knowledge through the SECI model.

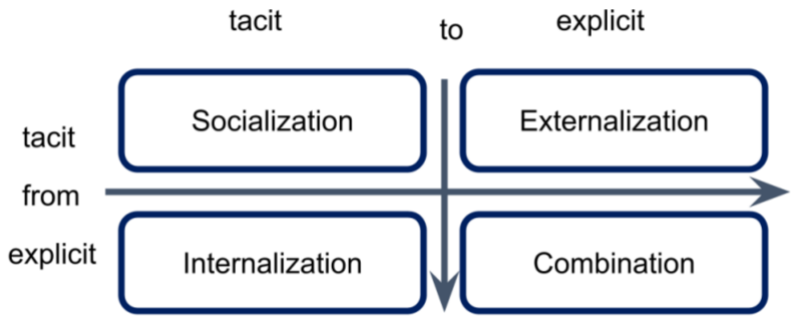

Figure 2.4: Four modes of transferring knowledge in the SECI model (Nonaka & Takeuchi, 1995).

Socialization refers to transferring tacit knowledge of one individual to tacit knowledge of another person (North & Kumta, 2018). For example, when a newly hired employee learns from a senior employee through observation, imitation and practice. According to North and Kumta (2018), articulating tacit knowledge into explicit concepts is called externalization. This emerges, e.g., when documenting manufacturing processes for the purpose of an ISO-certification. While externalization only reveals a part of the tacit knowledge, it serves as valuable references. However, externalization should not be relied on solely. Instead, involve employees with first-hand experience for deeper understanding. Externalization is the basis for reflecting experiences, formalizing learning processes, and also standardization and process improvement. Combination is the process of converting from explicit knowledge to explicit knowledge (North & Kumta, 2018). This entails individuals exchanging and combining knowledge by the means of documents, meetings, and communication networks. Existing information is reconfigured through sorting, adding, combining, among others, potentially generating new information. The combination of explicit knowledge to explicit knowledge often follows an economic of reuse and serves as the foundation for innovation, and incremental improvement of products and processes. Internalization involves the incorporation of explicit knowledge in tacit knowledge, which is closely related to learning by doing (North & Kumta, 2018). For instance, a service engineer may read a manual of how to program a machine.

The SECI model has faced critique in management and organizational studies, as summarized by Easa (2012). Nonaka and Takeuchi (1995) tend to regard tacit and explicit knowledge as two distinct entities, where knowledge is either tacit or explicit, with no in-between. However, this perspective has been criticized for not recognizing that tacit and explicit knowledge should be viewed as complimentary entities. As previously said, all tacit knowledge may not be converted to its explicit form. Additionally, this also expects to limit the effectiveness of the externalization process (Easa, 2012).

3. Method

The following section describes the research strategy and design, data collection and thematic analysis in this thesis. Furthermore, research quality and ethical aspects are also described and considered.

3.1 Research Strategy and Design

For this study, a qualitative research design was chosen, which is a research strategy that prioritizes words and images rather than quantification in the collection and analysis of numerical data (Bell et al., 2019). Furthermore, a qualitative approach is often used in business and management studies and is suitable for generating theories (Bell et al., 2019). According to Bell et al. (2019), a case study is commonly used for intensive examination of a defined system, i.e., the internal audit process. Furthermore, the case study should be selected based on the potential of learning opportunities. Bell et al. (2019) also suggest that case studies provide a use of several qualitative methods, where interviews, observations and documentation of company data can be combined to avoid reliance of a single method.

3.1.1 Case Study at the Swedish Transport Administration

The Swedish Transport Administration (STA) is a public organization driven and financed by the Swedish state. Furthermore, the organization consists of 9,000 employees with headquarters located in Borlänge, Sweden. The organization is responsible for the long-term planning of the transport system within the areas of road, rail, shipping, and aviation. Responsibilities also include building, maintaining, and coordinating these areas to ensure an effective infrastructure that promotes safe and environmentally sound traveling within Sweden (Swedish Transport Administration, 2024b). The organizational structure of the STA is illustrated in Figure 3.1 below.

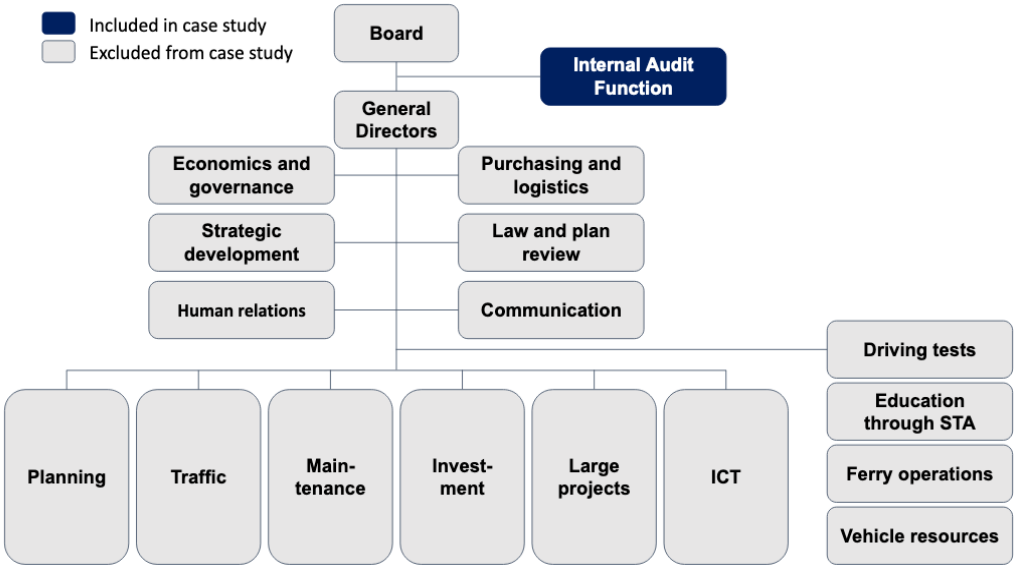

Figure 3.1: The organizational structure of the STA. Translated and adapted from the Swedish Transport Administration (2024b).

The study has been conducted within the STA internal audit function consisting of 11 internal auditors and a chief auditor executive, located in different cities of Sweden. The internal audit function serves as a complement and support to ensure reliable internal control within the organization. The internal audit provides objective and independent audits and advice, contributing to continuous improvements and the capability of the organization to meet requirements and achieve goals. In the upcoming year, the internal audit function has the resource capability to perform 12 audits (Swedish Transport Administration, 2023). The audits should be based on analysis of the organization's risks and aims to ensure that the organization's internal control is established and performed in an appropriate way to fulfill the Swedish law for authority regulations. Furthermore, the internal audit function also needs to ensure that obligations associated with the Swedish membership of the European Union are considered and complied with. Additionally, the reporting should be reliable and authority assets managed efficiently. Moreover, the auditors are required to ensure objectivity by conducting independent audits of the organization and adhere to established internal audit practices (Swedish Transport Administration, 2021).

The role of the internal audit function in relation to the operations of the STA can be explained through the framework Three Lines of Defense (The Institute of Internal Auditors, 2020), which is depicted in Figure 3.2 below. The framework describes how responsibility of risk management is delegated between three different groups, or "three lines", of an organization (The Institute of Internal Auditors, 2020).

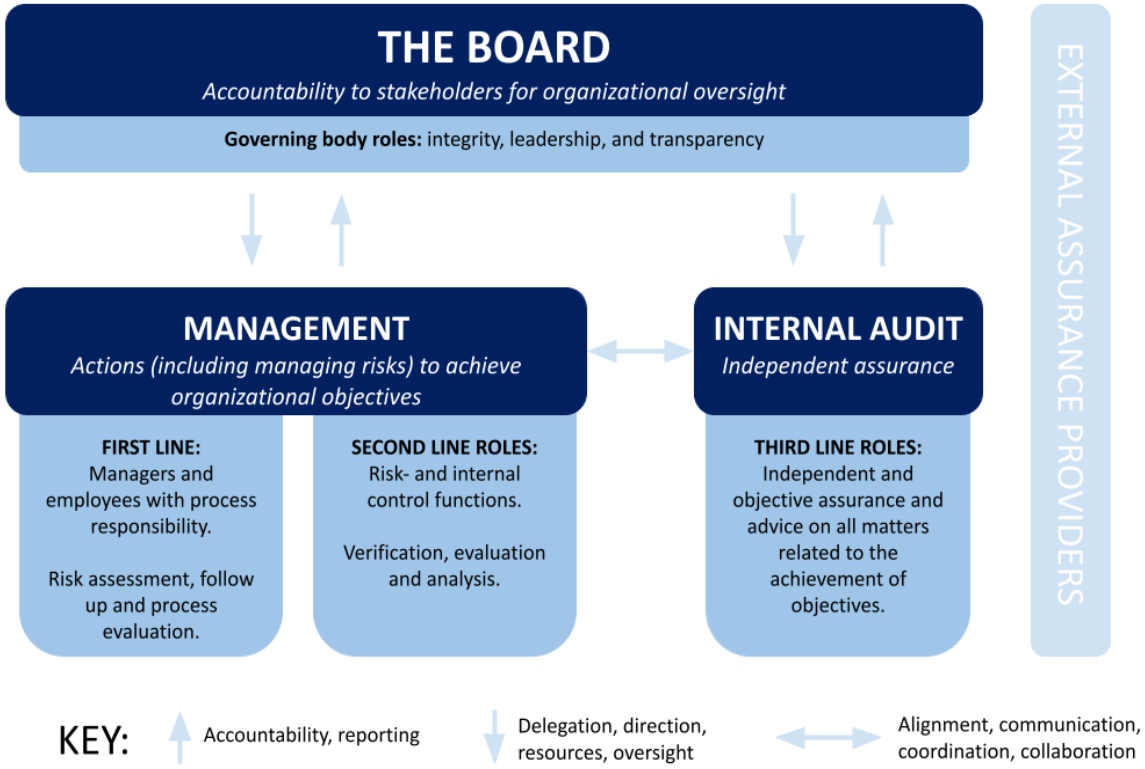

Figure 3.2: The role of internal audit in relation to operations of the STA. Adapted from The Institute of Internal Auditors (2020).

The first line is mainly composed of business operations and operational management, which is responsible for managing and owning risk day to day. The second line controls and oversees risks to ensure that the first line operates effectively. Furthermore, the second line consists mainly of functions like risk management and internal control. Lastly, the third line is the internal audit function which aims to provide independent and objective assurance on all matters related to the organizational objectives. Additionally, the internal audit function mainly evaluates the first and second line independently. Above the three lines is the governing body, the Board of STA, which guides and communicates expectation to the three lines of defense. External auditors and regulatory authorities operate outside of the structure, but these assurance providers may perform independent assessment of either the whole, or parts of the organization (The Institute of Internal Auditors, 2020).

The case study aims to contribute to the continuous improvement of the audit engagement process, with an essential focus on the engagement planning. The study should provide recommendations on how to improve the process including suggestions on how to implement the recommendations. Furthermore, the study should present a practical model, supporting the auditors to effectively and systematically focus the effort towards highly prioritized areas. The result should be based on following:

- Relevant theory in relation to internal auditing
- Existing knowledge and experience within the internal audit function, and also with specific adaption to the STA requirements
- Analysis and evaluation of possible prioritizing models for achieving an effective and appropriate engagement planning.

3.2 Data Collection

The primary data collection methods employed were review of company documentation, observations, interviews and a literature review. Reviewing company documentation created a basis for answering RQ1. To create an additional and expanded perception of the internal audit process and to facilitate answering all research questions, observations were done. Furthermore, interviews were conducted to obtain an understanding of an internal auditing process performed in practice and were used to address all three research questions. Lastly, a literature review was produced to create an understanding of current theories and concepts within the area of research.

3.2.1 Interviews

Interviews were conducted in two different phases. The first phase involved explorative interviews and the second phase consisted of semi-structured interviews. All interviews were conducted digitally through Skype as it was convenient for both the researchers and the interviewees due to geographical constraints. All interviews were recorded, transcribed, and later analyzed, except for two interviews where notes were taken and analyzed.

Exploratory Interviews

According to Adams (2007), explorative interviews can be utilized to define the scope of research, which is critical to successful research. This includes the formulation of the problem. Part of formulation in business research is to interview relevant stakeholders to explore and understand what subjects are important (Adams, 2007). In this study, four explorative interviews were conducted and three were recorded, each lasting between 45 to 90 minutes. These interviews were held to gain a general understanding of internal auditing at the STA, both the methods and the process as a whole. Additionally, through these interviews, further areas of interest to the research questions were identified and formed the basis for the semi-structured interviews.

Semi-structured Interviews

A common strategy for collecting qualitative data is through interviews (Bell et al., 2019). The interviews were conducted in a semi-structured way. This is a suitable approach when collecting qualitative data in an open-ended way, and to get an in-depth understanding of an issue (Bell et al., 2019). A semi-structured interview allows the interviewers to deviate from the interview guide to explore interesting viewpoints that may arise during the interview (Bell et al., 2019). Before conducting the semi-structured interviews, an interview guide was established (see Appendix A.1), consisting of open-ended questions. The questions were designed to both seek clarity of topics that were unclear and to explore areas of interest identified in the explorative interviews. Furthermore, questions were also formulated to further deepen the understanding of both methods and processes of internal auditing at the STA, especially the engagement planning. The prepared interview guide was adapted as needed to allow for new viewpoints that arose during the interview. All semi-structured interviews at STA lasted between 90 to 110 minutes and were recorded.

Furthermore, an additional interview guide (see Appendix A.2) was specifically prepared for an interview conducted with a top manager for a company working within internal auditing, having expert knowledge within the subject. The purpose of the interview was to create an understanding of the subject from an outside perspective, beyond the case. The interview guide was adapted from the original guide used to interview the internal auditors at the STA to focus on perspectives outside of the STA to ensure that the questions were relevant. Further, the interview sought to gain a broader understanding of internal auditing and how external perspectives might differ or align from the perspectives at the STA. This expert interview lasted around 60 minutes and was not recorded.

3.2.2 Sampling

According to Bell et al. (2019), purposive sampling is a common method for qualitative research. It is a non-probability sampling method where the interview selection is deliberate and purposeful, and not random. Thus, this sampling method will allow the research questions to be answered (Bell et al., 2019). The sample was selected strategically to allow for a broad understanding with the research questions in mind. In this study, a total of nine interviews were conducted with six participants, which is illustrated in Table 3.1. The respondents A-E are working at the STA and have different previous professional experiences and possess various levels of knowledge about

internal auditing and associated processes. Furthermore, the respondents had worked within the STA for different lengths of time. This led to a variation in the result, since the questions were answered from several perspectives. Furthermore, an external interview with a top manager within internal auditing was performed, which contributed an additional perspective from outside of the organization.

Table 3.1: List of interview respondents.

Respondent	Role	Type of Interview
A	Internal Auditor	Exploratory and Semi-structured
B	Internal Auditor	Semi-structured
C	Internal Auditor	Exploratory and Semi-structured
D	Internal Auditor	Exploratory and Semi-structured
E	Internal Auditor	Exploratory
X	Top Manager	Semi-structured

3.2.3 Literature Review

According to Bell et al. (2019) a literature review is done to create an understanding of what is already known within the area of research, including theories and concepts. However, the literature is supposed to be of a critical nature, meaning it should consider several perspectives of the topic and how it coheres to the research (Bell et al., 2019). In this study, a literature review has been carried out to establish a theoretical background of internal audit operations as well as continuous improvement methods, such as PDSA. The literature was retrieved from various online databases, such as Google Scholar, Chalmers Library, and Scopus using relevant search terms as shown in Table 3.2. These search terms were also combined, e.g., “internal auditing” AND “risk assessment”.

Table 3.2: Search terms used for the literature review.

Internal Auditing	Quality Management	Knowledge Management	Risk Management
Internal audit (IA) Internal auditing IA planning IA framework IA literature review Engagement planning IPPF	PDSA Quality management Continuous improvement	Knowledge management Knowledge management practices Tacit knowledge Implicit/explicit knowledge	Risk management Risk assessment 4T’s COSO ISO 31000 Risk based IA

3.2.4 Company Documentation

One way for collecting data is by analyzing documentary data sources e.g., websites and reports (Bell et al., 2019). This form of documentation is not created as a basis for research business, but the researchers can distinguish relevant data and how to analyze it as an extended data source (Bell et al., 2019). Documentation at the internal audit function of the STA served as a source of data. A review of documentation was carried out as a supplement for the conducted interviews to get an understanding of internal auditing, and how internal auditors work according to routines and documentation. The documentation reviewed in this research is summarized below in Table 3.3.

Table 3.3: Summary of reviewed internal auditing documentation within the STA.

Document (number of pages)	Description
Internal Audit Plan 2024-2026 (14)	- Summary of audits (total of 12) - Summary of significant risks (total of 14) - Description of audit objects
Internal Auditing Handbook (43)	- Description of overall internal auditing approach and methodology
Manual C2 Audit System (32)	- Procedures for documenting audits in the audit system
Board Guidelines for Internal Audit (5)	- Assignment description - How internal audit work should be applied in practice - Guidelines for good internal audit practices
Internal Audit Annual Report 2023 (26)	- Reporting and follow-up of audits - Audit statistics - Conclusions from conducted audits - Development and quality (operational changes)

Table 3.3 (continued).

Audit report 1 (12) “Management of private roads” Audit report 2 (20) “Facility information”	- The audit reports include information about assessed areas, scope and objectives, observations and recommendations, as well as risk assessment, among other. In short, the audit report is a summary of the audit work and aims to present the result.

3.2.5 Observations

Observation is another form of collecting data (Bell et al., 2019). In this research, meetings held during audits were observed to gain a deeper understanding of the dynamics of the audit team and the audited department. Specifically, observations were conducted during two meetings, with detailed notes taken on interactions between the audit team and the audited department. These meetings also provided an additional understanding of the audit process.

3.3 Thematic Analysis

Thematic analysis is a qualitative data analysis which, as the name suggests, entails searching for themes in the interview data (Bell et al., 2019). According to Ryan and Bernard (2003), a common criterion for a theme is repetition, i.e. repetitive topics, that are recurring in the interview data. In this thesis, the interviews were transcribed and analyzed to identify and find patterns that are relevant to the research aim. Firstly, the recorded interviews conducted with internal auditors at the STA were transcribed enabling coding of interview data that was relevant to the aim of the research. Each transcript was coded one at a time which involved re-reading the transcript to get an overall sense of the information. Next, the data was examined and broken down into meaningful codes that reflected the content, in order to categorize the data. Subsequently, similar codes were then later grouped, forming broader themes that were relevant to the research questions (see Figure 3.3).

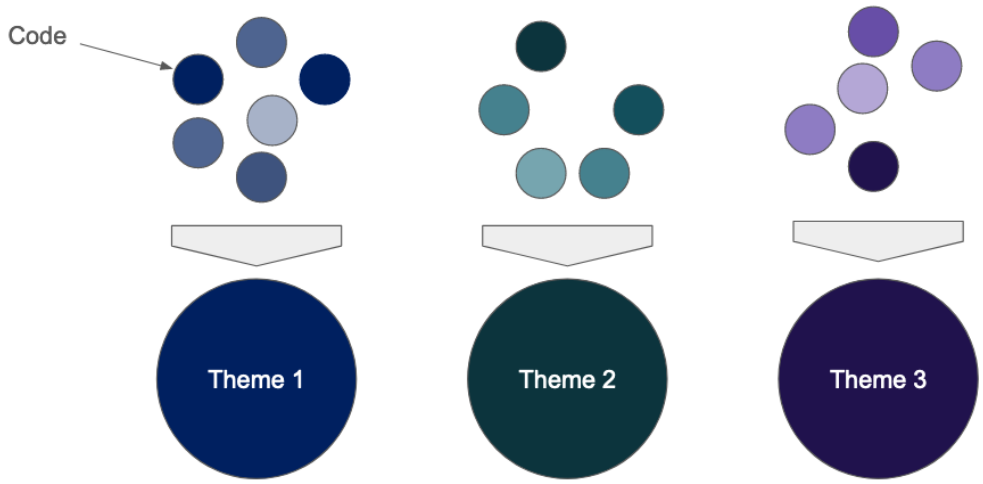

Figure 3.3: Illustration of the thematic analysis

3.4 Research Quality

In qualitative studies, assessing the quality of research involves examining its trustworthiness. Trustworthiness is evaluated in four areas, including *credibility, transferability, dependability,* and *conformability* (Bell et al., 2019). The following section aims to describe the quality of research of this study.

3.4.1 Credibility

Bell et al. (2019) identifies credibility as the first criterion of trustworthiness. Credibility involves ensuring that the research follows good practice and accurately represents the social setting being studied. In confirming the accuracy of findings with participants, the researchers can also confirm that the research is correctly understood. In establishing credibility, several techniques can be used, such as triangulation and respondent validation (Bell et al., 2019). Triangulation involves using several methods to collect data which enables cross-checking of data sources against each other. Respondent validation includes ensuring that there is a good correspondence between the findings and the perspectives and experience of the research participants (Bell et al., 2019). To increase the credibility of this study, triangulation has been used to confirm the findings through cross-checking several sources of data such as interviews, observations and documentation. Furthermore, during interviews the researchers posed questions seeking to confirm and validate that the perspectives shared by the interviewee were correctly understood.

3.4.2 Transferability

Transferability is the second criterion of trustworthiness presented by Bell et al. (2019). Transferability examines to what extent the research findings can be applied or generalized to other contexts. Qualitative studies tend to focus on the unique characteristics connected the researched phenomena and may therefore not be applicable in a broad context (Bell et al., 2019). However, as a means to increase the transferability, a “thick description” may be produced, including a rich and detailed description of the context. Thus, other researchers can assess whether the findings may apply to their own setting (Bell et al., 2019). In this study, a “thick description” has been provided to increase the transferability of the findings. However, in those cases where the findings may not be generalized, it may still serve as a good example.

3.4.3 Dependability

The third criterion of trustworthiness is dependability according to Bell et al. (2019). Dependability is comparable to reliability in quantitative studies and examines whether the research methods can reproduce or replicate the same findings. In qualitative studies, Bell et al. (2019) presents the “audit” approach which can be used to determine the dependability. This involves keeping complete records of all processes throughout the study, and then, preferably, towards the end of study having peers to act as auditors, reviewing whether the process has been followed or not (Bell et al., 2019). To increase the dependability in this study, a thorough documentation of the research process was produced. The documentation includes, e.g., transcripts from interviews, procedure of the data analysis, among others.

3.4.4 Confirmability

Finally, confirmability refers to the assurance of objectivity within business research (Bell et al., 2019). Although it is not possible to achieve complete objectivity, it should be expected that individual values are not included in the study and that the researchers strive to attain objective results (Bell et al., 2019). In this study, the interviews were conducted and analyzed jointly by both researchers to enhance the understanding of the material. Several interviews were recorded, which made it possible for the researchers to review the material repeatedly and discover potential misconceptions. Furthermore, several sources of information were analyzed and compared, to increase a broader perspective on the matter.

3.5 Ethical Aspects

The ethical aspect of business research corresponds to the responsibility, carried by the researchers to protect the participants from harm (Bell et al., 2019). There are four ethical perspectives associated with business research; informed consent, prevention of harm, confidentiality and avoidance of deception, according to Bell et al. (2019). This section will present three perspectives in which the thesis will show consideration for.

3.5.1 Informed Consent

According to Bell et al. (2019), to ensure informed consent, the participant should be provided with sufficient information about the study. The participant must be able to decide based on this information, whether he or she wishes to participate of his or her own free will. In addition, it is also essential how it is presented and that the participant is given enough time to feel comfortable with their choice (Bell et al., 2019). As part of this work, participants were provided with written information about the study and its purpose. Furthermore, the invitation for the interview consisted of information regarding the respondents right to avoid answering certain questions and the right to interrupt participation at any time, which allowed the respondents to participate voluntarily. Interviews conducted as part of the study were recorded to prevent loss of valuable input. However, this was only done if the participant consented by confirming before each interview.

3.5.2 Prevention of Harm

Harm can appear in a variety of forms and can be both physical and psychological in nature. According to Bell et al. (2019), preventing harm can be directly connected to maintaining anonymity and confidentiality, stressing that identities should be treated with care. Furthermore, Bell et al. (2019) states that it can be difficult to predict if harm to participants will occur, however, the importance of trying to protect the participants remains. Because the sample size for this study is relatively small, participants will only be introduced on a general level and referred to by letter in order to maintain anonymity and minimize the risk of exposure to sensitive information. To further reduce the risk of exposing identities, the internal audit function at the STA requested that quotations should not be assigned to a specific internal auditor. Therefore, the citations will only refer to the respondent’s role instead of their assigned letter.

3.5.3 Confidentiality

Confidentiality refers to the anonymity of the participants, preventing exposure of identity to protect the participants from judgment by the company (Bell et al., 2019). As with informed consent, it is equally important to protect the privacy of participants (Bell et al., 2019). To reinforce confidentiality, the respondents will be given the opportunity to cancel the participation and avoid questions that they don't feel comfortable answering. According to Bell et al., (2019), confidentiality can appear in the form of an agreement with the company, established to limit the researchers from accessing or sharing specific information. However, for this study it was decided by the chief auditor executive that this type of agreement was not necessary.

4. Results and Analysis

Internal auditing at the STA is described in Section 4.1 to provide an overview of its documented processes and practices. Section 4.2 is based on interviews conducted with internal auditors at the STA, and outlines identified themes from the thematic analysis. Furthermore, these themes are concerned with how internal auditing is performed in practice. Subsequently, both Section 4.1 and 4.2 are compared to identify parts of the process that lack clear instructions on how to perform certain activities, which is presented in Section 4.3. Finally, in Section 4.4, results from the external interview are presented and serve as an outside perspective in contrast to internal auditing practices within the STA.

4.1 Documented Internal Audit Process

This section aims to describe the process of internal auditing at the STA according to company documentation to provide a general understanding of practices conducted by internal auditors. Furthermore, this subsection aims to form a basis in order to address RQ1: *How does an internal audit function perform an audit in practice, and how is the audit process described in documentation?*

4.1.1 Annual Audit Plan

Once a year, the internal audit function at the STA participates in a two-step process to form an audit plan for the upcoming year. The process consists of two meetings, where the first meeting includes a risk analysis, where risks to the entire organization are identified, analyzed and prioritized. This forms a base for the second meeting, where the most critical risks are determined, resulting in audit engagements presented in the annual audit plan. The plan should include a direction and an overall purpose for each audit engagement. Creating an effective audit plan is characterized by flexibility and management support. The audit plan can continuously be revised with updated information until the board approves and formally establishes the plan. Afterwards, the chief auditor executive distributes audit engagements to the internal audit team. Often, a single engagement is carried out by two internal auditors, where one is designated to be lead auditor.

Connected to the annual audit plan are several surveillance areas in which the responsibility is divided between the employees. The purpose of the surveillance areas is to identify potential risks, serving as a foundation for upcoming audits. The areas are shared with one or several colleagues and aims to streamline internal audit activities by increased long-term knowledge and continuous learning. Responsibilities within the surveillance areas include learning about overall findings, external monitoring, and establishing an internal and external contact network within the specific area. This enables for knowledge being passed forward to the other colleagues, creating an environment for the employees to learn from each other.

4.1.2 Internal Audit Engagement Process

The audit engagements at the STA are generally executed over a period of nine weeks, which are divided into four different blocks (Figure 4.1): planning, implementation, quality assurance, and follow-up. An audit engagement is generally conducted by an audit team consisting of two internal auditors, where one is chosen as lead auditor.

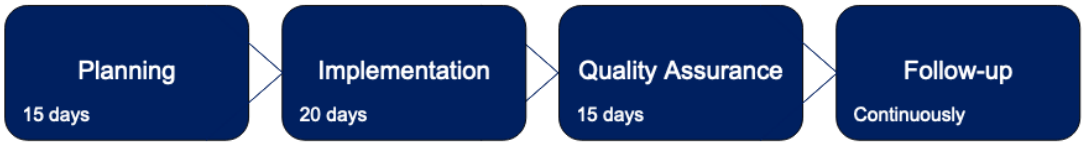

Figure 4.1: Audit engagement process within the internal audit function of the STA.

Engagement Planning

Planning is generally carried out for three weeks and involves defining the purpose and scope of the audit project. The planning phase aims to provide the audit team with a better understanding of the area to be audited. Furthermore, communication is a critical success factor during the planning phase and provides a good basis for cooperation and open dialogue throughout the audit engagement.

Initially, the lead auditor prioritizes establishing communication with managers (e.g., Head of Operations) of the departments to be audited. The lead auditor receives a list of persons to contact, provided by the appointed audit coordinator. This enables the audit team to plan upcoming meetings with the managers of the audited department, which is essential in the planning phase to prepare and maintain consistent communication. The audit team also establishes a standardized project structure and working environment to support various stages of the audit, e.g., creating documents such as auditing program, a time scheme for the program, and a planning document, which is continuously processed throughout the engagement planning. The audit program is usually ad-hoc and aims to create guidance throughout the audit engagement to demonstrate completed audit activities. The time scheme for the audit engagement describes the chronological order of activities to be carried out. Lastly, the planning document is the working paper, which is continuously developed by the audit team, aiming to create a uniform perception of the audit engagement. Contents of the planning document is based on the risk analysis, the audit plan and a supplementary risk analysis performed by the audit team.

Internal planning meetings are held early in the planning process. All of the internal audit staff is invited by the lead auditor to contribute with their expertise to plan the audit. These meetings include discussions related to engagement planning where the audit team can benefit from the competencies from their colleagues within the internal audit function. Furthermore, these meetings can be held multiple times depending on the audit's complexity. For example, the purpose, scope of the audit and potential interviewees are areas that may be discussed. Separate planning meetings are also held with managers of the departments being audited, with the intent to receive further input regarding e.g., business context and ongoing development initiatives. Furthermore, the audit team plans for upcoming meetings such as the opening meeting and end meeting. Before the planning phase ends, an opening meeting is held with

representatives of the audited department to present the intended scope and approach for the audit engagement, stemming from the planning document. During the meeting it is possible to further adjust the scope to ensure alignment of expectations.

Implementation

The next step in the internal audit process is the implementation, which is characterized by critical analysis, active discussion, and a high degree of proactivity. The scope of the audit is flexible, and adjustments can be made during the entire engagement process. The lead auditor is responsible for dividing the work equally between those involved in the engagement. During the implementation phase, introductory meetings is a common practice and are usually held with several participants at once for efficiency reasons. These introductory meetings are often held when conducting site visit at the workplace, and the topics covered are similar to the contents in the opening meetings.

Observations should be described clearly and concisely to facilitate the identification and understanding of risks. This includes defining both the desired and current state, identifying the root cause of current conditions, and conducting an impact assessment. According to routines, it is important to analyze the cause of the observation as it guides both risk and recommendation. A method that is utilized for finding the root cause is Toyota's Five Why's, which is performed by asking the question *"why?"* five times. As observations have been identified and documented, internal auditors use the STA risk assessment matrix to evaluate the risk of these observations. The risk assessment is based on residual risks, meaning the assessment is made with consideration to the controls already set by the business, aiming to manage and minimize the risks.

Activities are assessed based on two criteria. The first criteria aim to reflect the effectiveness and efficiency, i.e. are the right things done in the right way. The second criteria should reflect the applicability to determine if the work methods applied are suitable to achieve set objectives. To achieve an effective management system requires appropriate activities that is conducted correctly. An effective management system consists of effective activities that are complied with. However, in instances where acceptable net risk is not achieved due to a lack of appropriate activities, the internal auditors focus on management´s actions to develop, improve and implement activities. Furthermore, where acceptable net risk is not mitigated due to non-compliance, the internal auditors should focus on management's follow-up of implemented activities.

In managing risks (see Figure 4.2), the goal is rarely to eliminate risks as there are few activities that can or should be conducted without risks. Nevertheless, it is important that the organization comprehend the current risk level.

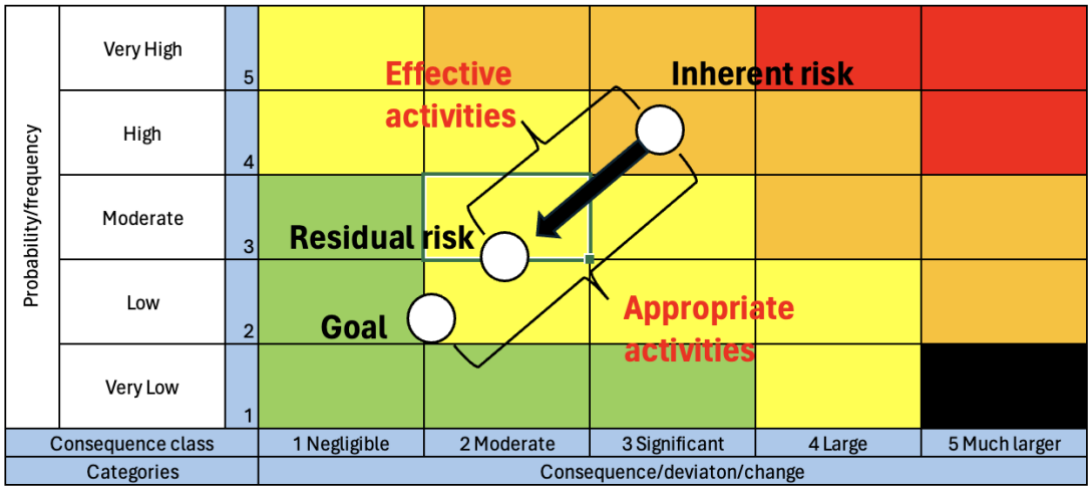

Figure 4.2: Illustration of risk matrix for assessing risks (Swedish Transport Administration, 2024a).

There are five assessment levels for observations, including very low, low, moderate, high, and very high. The level is set when the audit is conducted and cannot be changed while the engagement is ongoing.

Furthermore, the internal auditors should provide the audited business with recommendations on appropriate actions to take for the business to achieve the desired position. In addition, an assessment of the entity´s ability for internal control and governance is made as a base for the result. A developed model, including different criteria, is applied to conduct this assessment and it should result in a common conception of the audited business. Finally, to conclude the implementation, an audit report is established including the result of the audit.

Quality Assurance

To achieve successful audit results which contributes to the organizations improvement work, communication and collaboration is of great essence. Therefore, a quality assurance is conducted for the project, enabling the organization to contribute with opinions and input. A draft of an audit report is finished and distributed to the organization followed by an end meeting held to ensure that the audit report is formulated so that the message is interpreted correctly by the receivers. The report is, if necessary, revised with adjustments from the organization before it can be established and communicated to the participants.

The internal auditing function presents the audit report, and the audited department can choose to accept the risks or to report back to the internal audit function with a suggested action plan for managing the observations and recommendations presented by the internal auditing. The action plan should cover risk owners, activities and a timetable. For the more extensive action plans, ranging over a year, it should also present partial deliveries to facilitate the follow up for the audit team. Once the action plan is delivered to audit team, the internal auditors is responsible for assessing the suggested actions whether the risks are controlled within the observations. To conclude this stage, if the risks are properly controlled, the action plan is approved.

Follow up
Lastly, an effective follow-up is of importance for the internal audit function. With each audit engagement, the lead auditor is required to make continuous follow-up on the actions made by the audited business for improving the observations. Before a follow-up, each auditor will get a notification to create a status update in a program called C2. The update is done three times a year and is based on the action plan previously suggested in the audit report. The assessment for the follow-up includes the findings of the audit, in combination with the improvement actions taken.

4.2 Internal Audit Process in Practice

The following chapter outlines themes identified from the thematic analysis, based on the in-depth interviews. The analysis resulted in several identified themes: Annual Audit Plan, Engagement Planning, Feedback, and Individual knowledge. These themes are relevant to answer RQ2: *How can an internal audit function strengthen risk management in engagement planning?* and RQ3: *How can an internal audit function adopt knowledge management practices to improve audit engagements?* Furthermore, some of the sections also include subsections. Additionally, it is important to note that internal auditors perform audits according to the process outlined in previous chapter. These themes aim to shed light on activities of internal auditing which lack clear instructions on how to perform, especially within engagement planning.

4.2.1 Annual Audit Plan

When the internal audit function forms the annual audit plan, risks are compiled both from the organization's risk management system (PULS) and risks identified within the different surveillance areas. A common way for assessing these risks is by using the STA risk assessment matrix. Additionally, other aspects are also considered in the assessment of risks to create a balanced annual audit plan, e.g., timing, coverage of the organization, previous audits and whether the risks are still relevant.

"We can't just take our risk map [the STA risk assessment matrix] as it is and say that we need to revise all of it; there are other parameters taken into account as well."
- Internal auditor

"Feasibility has been considered [...] the risk, and the timing, is the time right?"
- Internal auditor

According to respondent A, there is a number of surveillance areas produced to cover the STA business as a whole. Within each area, a joint risk list is created and also a list of potential audits for the annual audit plan. Furthermore, the risks from all areas are later discussed in a meeting with the entire internal audit unit, where they become assessed and clustered. Respondent A mention that the number of risks is often too many for the unit to handle in one session and because of that, a limit for the risks were set for each surveillance area to make it manageable.

"I think we had over a hundred risks that we were supposed to go through in one day. It was completely impossible, so we slimmed it down to maybe five risks per surveillance area. [...] So that we had a more manageable amount."

- Internal auditor

The approach for risk analysis has, according to respondent C, been conducted in different ways but can be described as a session where the internal audit function compiles a risk list.

"It has perhaps been a slightly different approach to the actual risk analysis, so to speak, but essentially a day when we process this material and actually produce a risk list for the internal audit department."

- Internal auditor

Subsequently, essential risks are selected from the compiled risk lists which forms a foundation for potential audit engagements in the annual audit plan. However, assessing risks to identify essentials risk are, according to respondent A, described as unsystematic.

"I would say that there is no systematic approach to this work [the identification of essential risks]. I would like to see that there was".

- Internal auditor

As a result of this session, several audit engagements are defined, in terms of audit scope and connected risks, and presented to the board which determines 12 audit engagements to be included in the annual audit plan. However, respondent C mentions that these audit engagements may be too broadly defined.

"[...] but on the other hand, you can think about whether we should perhaps work on developing our audit engagements in the annual audit plan a little more crispy [well-defined] than they are perhaps in some cases today. Overall, this works quite well, I would say."

- Internal auditor

4.2.2 Engagement Planning

Scope and Limitations

The audits in the annual audit plan are based on risks. Several respondents (A, B and C) mention that those risks are used in the planning phase where a supplementary risk analysis is carried out. Respondent B emphasizes the importance of conducting the supplementary risk analysis to see if the risks are still relevant and to expand the knowledge from the more basic analysis made when conducting the annual audit plan. Furthermore, respondent A and C both describe the supplementary risk analysis as an unsystematic task.

"Based on the risks of the business and our own annual risk analyses, we have not done much more. We have not really analyzed them, I think. [...] But we probably

work very differently with the analysis. We probably try as best we can, but I think it would be good to have some more points to stick to there too"

- Internal auditor

"So yes, we do some kind of additional risk analysis in the planning stage of the specific audit. Then exactly how systematic it is can perhaps be considered."

- Internal auditor

According to respondent A, in distinguishing the most essential risks in the supplementary risk analysis, it is possible to form a base for assessment criteria and orientation for the audit engagement. Furthermore, respondent D mentioned the importance of looking for additional risks and if the business part being audited has any new information about emerging risks. This view is also shared and expanded upon by respondent C, which also suggests reviewing the status of the identified risks, either from the business or internal audit function, and finding the desired position. This may also include search for existing action plans and being aware of influencing factors from the external environment.

According to respondent B, the limitations are adjusted so that they fit within the time given for an audit engagement. If the engagement formulated in the annual audit plan is perceived as too extensive, the project will be narrowed down. Furthermore, respondent C expresses that audit engagements from the annual audit plan are sometimes too widely formulated and, in those cases, unmanageable to complete within the time given for the audit engagement. However, respondent C notes that setting limitations too narrow is not always possible and there should be some flexibility throughout the engagement. Respondent A also brought up the wide description of the audit engagements and mention that there are seldom any large changes on those formulations.

"Then you might think that there is perhaps a problem that sometimes we have something that is quite broadly formulated in an audit plan and then we do it, then we delimit it in the planning of individual objects [engagements] quite tightly. […] But on the other hand, I would like to say that there has never been anything that has come back. I don't even know if the organization has had any views on it like that."

- Internal auditor

After setting limitations for the engagement, respondent D reflects around if the limits are set on an appropriate level given the time restrictions. Moreover, since an audit can cause concern within the reviewed unit, presenting clear expectations for the audit becomes essential. Since the annual audit plan has been approved by the board, it becomes important that the audit scope does not diverge from agreed expectations for the audit engagements.

"*[…] Because that's the audit plan, that's what we have to relate to, and you can't go outside that description and audit something completely different, because this is the audit plan, which is the Board's wishes for what should be audited in the next year.*"

- Internal auditor

Formulating Audit Questions

Several respondents (A, C and D) mentions that there are usually a few audit questions formulated in the beginning of an audit. These questions are based on identified risks associated with the audit and is supposed to be answered when the audit is completed. The number of questions seems to be varying but according to interviews, it usually ranges somewhere in between one to four. Respondent A thinks that a maximum of two questions is appropriate to find the root cause for the risk while staying within the scope of the engagement, also considering there is a limited amount of time to complete the audit engagement. Respondent C also expressed that:

"The audit questions, they clearly set some kind of limitation. But we probably have and maybe should have some flexibility anyway because, as I said, something may come up that we completely overlooked or at least downplayed a lot in the planning."

- Internal auditor

When planning an audit engagement, respondents B, C and D emphasized the importance of the desired position, referring to what the audit is intended to result in. It is necessary to consider what the desired position is to be able to evaluate the organization. In this process, clearly defined boundaries and audit criteria is important according to respondent D.

"But I would say that of course you start from what there is... somewhere try to look at some kind of standards or regulations in a field. What is the desired state or what are we revising towards? To reflect on it."

- Internal auditor

Expanding Knowledge in Planning Meetings

As previously mentioned, planning meetings are held early in the internal audit process together with the internal audit team and with managers of the function to be audited. In this meeting, the internal audit function has the opportunity to both understand the area to be audited better and receive feedback from the department undergoing the audit. The structure for this meeting can differ from audit to audit, and auditors are relatively free to arrange the meeting as preferred. However, several respondents mentioned that being prepared for this meeting is key to receive valuable input or constructive criticism from the department undergoing the audit.

Respondent D strives to initiate and engage in discussion at this meeting believing this can yield a better audit result. Respondent D also emphasizes that reaching a consensus with the audited department on the scope of the audit engagement is vital to ensure that the department does not oppose the audit at a later stage.

"Because you want to, I mean, I strive for some kind of dialogue/discussion because I believe that the product [audit engagement] becomes better as a result."

- Internal auditor

Respondent A experiences that participation in discussions may vary depending on the audit engagement, and its relevance to the audited department. Additionally, reviewing an area where the department sees the need for improvement may flourish

the discussions. Respondent A also notes that some audit engagements are more interesting by nature, thus generating more active meetings.

"Certain topics are probably more interesting by nature, but I still find that there is always a professional attitude where people try their best to contribute."

- Internal auditor

4.2.3 Feedback

The internal audit function performs targeted interviews on a yearly basis with a careful selection of relevant people, often managers, that has been previously audited and whom has been heavily involved in the audit engagements. Subjects brought up to discussion revolves mainly around communication, quality of reports, and so on, according to respondent C.

“This allows the operations to provide feedback to us. We have been doing this for, I think, two years now, and it is a working method that we find beneficial.”

- Internal auditor

As of recently, this is the new way of collecting feedback from the audited departments, replacing the previous approach of conducting surveys, which was sent out after every completed audit. Respondent D expresses that those surveys became dull, and interviews serves as a more meaningful method for collecting feedback. Interviews allow the internal audit function to go in-depth and to achieve an understanding of different perspectives. In contrast, respondent A stressed that surveys only provided the internal audit function with feedback of an audit at a general level and believes that the audited function also prefer interviews over surveys.

"During these interviews, we don't engage in arguments; we really listen. We ask questions and take in their perspectives. [...] Our assessment is that this approach provides much more value than our previous surveys."

- Internal auditor

Respondent D mention that these in-depth interviews does not concern an individual audit engagement specifically. Instead, it revolves around how the internal audit function is perceived, more at a general level and improvement perspective.

4.2.4 Continuous Improvement

After finishing an audit engagement, the team evaluates different areas of their work through a standardized evaluation method. The team reviews both the positives and negatives of their work, e.g., the different phases of the internal audit process, and strives to identify areas of improvement. This serves as a basis for their quarterly improvement meeting, held together with the entire internal audit function. In this meeting, the discussions revolve mainly around what the internal function can do to improve its processes. In the case of any identified improvement in their ways of working, it is documented in their routines, given that the entire internal audit function is in an agreement.

“We have a 10-minute evaluation that we usually conduct after the final meeting, where we review the different parts, consider if the purpose has been fulfilled, assess how the planning has progressed, and identify areas for improvement.”

- Internal auditor

Respondent D stresses that it is important to remain open to changes, and loyal to the improvements made. This is especially true for the internal audit function as they do audits and identify risks that need to be managed and dealt with, which can include new ways of working. Respondent D adds another viewpoint that if the internal audit function is not willing to change and improve, there may be less commitment for the audited function to do so as well.

"And if we don't have that approach ourselves, it is very difficult to go out to the audited department and tell them that they need to change if we ourselves don't have the ability to change, so it is very important."

- Internal auditor

Respondent B acknowledges that one of the dangers in working with internal auditing and managing risks is that the internal audit function stagnates in its ways of working, believing that an optimal method has been found. Instead, respondent B thinks that the internal audit function must continuously work to improve its approach.

“In my experience, the most dangerous thing in risk work is to stagnate and say that we have now found the optimal model for risk analyzing the business.”

- Internal auditor

4.2.5 Individual knowledge

Respondent A expresses that the internal audit function historically mainly consisted of experienced internal auditors, with longer backgrounds at the STA, being very reliant on their gut-feeling and intuition guiding their work. As of lately, the internal audit function is more disparate, consisting of both experienced internal auditors and fairly new recruitments, having different backgrounds. Respondent A emphasizes that this creates a need for a more common way of working, as some parts of the process are dependent on individual ways of working. Respondent B also supports the view that there is work to be done to make processes less dependent on individuals.

“I think it [ways of working] has been quite dependent on individuals. I haven't felt there has been any clarity on how to think […] So, I would say that there is nothing that dictates how we should do things; instead, it is more about intuition and experience guiding us.”

- Internal auditor

On the note of individual ways of working, respondent D described some of their current methods as vague and unclear, and further highlights the risk of not achieving the same results if a new team were to replace the existing team.

Assessing risks is an activity that has a specific approach, still, parts of the risk assessment is reliant on experience and intuition according to respondent D.

> *"Risk, of course, feasibility, and perhaps it even boils down to some sort of gut feeling. Here we are really dealing with opinions."*
> - Internal auditor

But in these circumstances, respondent D expresses the importance of having a supportive and collaborative culture, where information and knowledge can be shared.

> *"It's like we share information; we don't hold back or withhold any information or knowledge. Instead, we are, I think, quite supportive of one another and try to help each other as much as possible in all situations. And how do you achieve that? Well, it's the culture among us that makes this possible."*
> - Internal auditor

The auditing process does include activities that are specifically designed for sharing information and knowledge. For example, planning meetings is an activity where all internal auditors participate, including the chief internal auditor. In this meeting, a draft of the audit engagement can be presented, however, the draft does not need to be extensively prepared for presentation, it can vary depending on the auditor's progress in the planning. Furthermore, to aid in planning the audit, colleagues can contribute with their knowledge and expertise according to respondent B.

4.3 Comparison of Documentation and Practice

A comparison of documented instructions and activities performed in practice was performed in order to address RQ1. The documented audit processes of the STA are comprehensive and covers most of the process. It outlines a structured approach, from annual audit plan to follow-up, with activities and timelines for each phase. In analyzing the process, both from interviews and documentation, it is evident that the process describes objectives focusing on what to achieve. However, some activities lack instruction on how to achieve these objectives. Thus, activities performed in practice of the audit process is listed in Table 4.1 below, aiming to highlight activities which lack clear instructions on how it should be performed. The highlighted activities are the following: define audit engagements, supplementary risk analysis, formulation of audit questions, and targeted interviews for feedback.

Table 4.1: Comparison between activities performed in practice and documented instructions of those activities.

Themes	Activities performed in practice	Documented instructions
Annual audit plan	Monitoring of surveillance areas	Clear instructions

Table 4.1 (continued).

Annual audit plan	Risk analysis	Clear instructions
	Define audit engagements	Lack of clear instructions
Engagement planning	Supplementary risk analysis	Lack of clear instructions
	Formulation of audit questions	Lack of clear instructions
	Planning meetings	Clear instructions
Feedback	Targeted interviews for feedback (yearly-basis)	No documentation to be found
Continuous improvement	Team evaluation after each finished audit engagement	Clear instructions
	Improvement meetings with all internal auditors (quarterly-basis)	Clear instructions

4.4 External Interview

This section includes the result from an interview conducted with an expert in the area of internal auditing, working at an external organization. This interview enables an additional perspective of the profession and process of internal auditing outside of the STA. Interview questions was formed to add on to the identified themes presented in Section 4.3, which facilitates in addressing the research questions.

4.3.1 Annual Audit Plan

According to respondent X, the annual audit plan are often based on a risk analysis. Some organizations also choose to include areas that are specifically in need of auditing that may have emerged from external audits or recent discoveries. Furthermore, the respondent also exemplified methods for conducting risk analysis in the annual audit plan, including a “Heat Map” which weighs likelihood of occurrence versus impact, as illustrated in Figure 4.3.

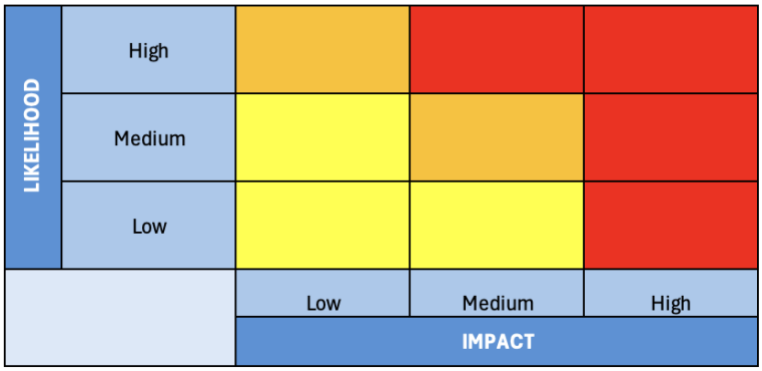

Figure 4.3: Heat map method in conducting risk analysis

Moreover, a risk analysis can cover verbal opinions or mathematical models. The respondent expands the reasoning underlining that the methodology used often corresponds to the design commonly used within each organization. On the note of risk analysis, respondent X highlights the importance of internal auditors doing a separate risk assessment, refraining from solely relying on the assessment made by the organization. Sometimes, the organization underestimate risks, and likewise, the internal auditors may occasionally overrate risks. For instance, the respondent X believes that risks connected to IT-security, fraud and corruption are frequently being underrated, while financial risks are often overrated. However, respond X emphasize the interest in how perspectives may differ. This could be due to the different risk orientations where the business units relate risks to their specific business, while internal auditors apply other aspect to it.

4.3.2 Engagement Planning

In terms of planning an audit engagement, respondent X mentions two approaches. Some internal auditors prefer to frame the project early in the process by allocating a large part of the time in the planning phase, collecting information, conducting interviews etc. On the other hand, there are internal auditors who prefer a shorter planning phase, where the planning is faster, and the process require more iteration. However, respondent X also underline that the approach can differ depending on the extent of the engagement e.g., if the area has been audited before and a pre-study is deemed unnecessary.

Connected to the engagement planning, respondent X brought up a personal experience of working with risk areas, going through previous known information, finding out if changes have been made or if new elements have been added since the formulation of the annual audit plan. Furthermore, risks might have drifted, and in those cases, a reassessment of the risk analysis is conducted since the initial risk assessment might not be relevant anymore.

According to respondent X, risks are usually classified, and there are several approaches to classification of risks, however, the preferred method tends to be closely related to the organizations overall model for risk classification. Respondent X also mention a concept called “audit universe” which is explained as an overview of the business used to select auditable areas. Additionally, the respondent stressed the

challenge of comparing risks, and understanding the significance of one risk compared to another, which can be even more difficult in a large organization as there are more risks to consider.

Respondent X sees a potential for improvement in the area of risk analysis, and further highlight that this activity is essential to succeed with internal audits. The respondent further argues that creating a dialogue with management is important to enable discussions regarding risk analysis. This entails discussing why the risk analysis is constructed a certain way and whether any changes need to be made, and also to be critical of the process. Respondent X explains that there can sometimes be quality managers involved continuously during the process, to discuss with. Additionally, asking for feedback from the audited unit and managers, to receive their perception of the process. The respondent also argued that an external audit reviewing the internal auditing department should be made each five years.

Audit Scope

According to respondent X, determining audit scope can be tricky and it is not unusual that it end up being too extensive, wanting to include more than possible to manage. In reviewing an area, opportunities to include additional elements often arise. However, further elaborating on an internal auditor being able to combine the broad perspective and narrowing it down, depending on if it is presented to the board or a business area manager. Furthermore, respondent X stresses the importance of formulating audit questions to facilitate the scope and extent of the audit, making it clearer. These questions should be put in relation to a number of criteria set to achieve the “desired position”.

4.3.3 Characteristics of a Successful Audit

The characterization of a well-conducted internal audit is, according to respondent X, that the stakeholders are pleased with the result and that the internal auditors has performed the audit professionally. The respondent continues by claiming that communication is essential, being able to communicate the accurate picture even though the perception is not always agreed on, set the basis for a good dialogue. Presenting evidence and staying relevant through the process are also signs of a successful result, according to respondent X. To add on to this, the respondent highlights the culture of internal auditing, and mentions the importance of open dialogue between internal auditors and the governing group, where input of emerging development areas can be suggested.

Connected to the performance of internal audits, the respondent mentioned key performance indicators and the difficulty of applying these within internal auditing. However, some examples were brought up e.g., number of performed audits, time for conducting the audit. The mentioned examples might be misleading and may fall outside of the quality aspect, since the result can depend on uncontrollable things. However, allocated time for conducting the audit is still an important objective to achieve, otherwise, the need for additional time should have been foreseen in the planning phase.

5. Discussion

5.1 Internal Auditing at the STA

RQ 1*: How does an internal audit function perform an audit in practice, and how is the audit process described in documentation?*

Presented in Table 4.1 are some discovered differences between the documented internal audit process at the STA versus how the process is performed in practice by the internal auditors. The analysis of Table 4.1 imply that identified differences in the process correspond to a lack of description, mainly focusing on what to achieve rather than providing instructions on how to perform specific activities. A strength in documentation is the structure, which is logical and coherent. Furthermore, findings show that the internal auditors at the STA are following the structure of the process and associated steps. However, the documentation occasionally lacks an explanation on how to perform the various activities, thus, each internal auditor may choose his or her own preferred method. This might indicate a low level of standardization, which may hinder continuous improvement over time. However, as mentioned by Gyllenhammar and Hammersberg (2023), standardization should not be the sole focus since it may hinder innovation. Hence, a lower level of standardization might have a positive impact allowing the internal auditors to be flexible, creative and learn from each other's practices as well. Furthermore, several respondents also emphasized the need for flexibility in the performance as it enables adaption of the specific audit engagement, yet some of the respondents still prefer a more systematic approach for selected elements of the process. Using equivalent methods for the same activity may lead to more consistent results of the audit engagements, however, the project can be of varying nature considering, e.g., area and size, which on the contrary require a flexibility in the process as well. Therefore, the internal audit function should strive towards a balanced level of standardization in order to maintain consistent results while still encouraging innovation, which support the holistic view of quality management mentioned by Kim et al. (2012). To achieve a balanced level of standardization, Ungan (2006) proposes that the personnel working with the process can contribute when determining the appropriate level of detail. Moreover, since the internal audit department at the STA currently consists of relatively few internal auditors it becomes natural to get inspired and learn from each other, thus there still seems to be a similar performance of the activities. There is a shared perception between internal auditors at the STA in terms of supporting one another.

Continuous improvement is an integral part of the internal audit function at the STA. Results are showing that there are several different meetings dealing with the improvement of the internal auditing process e.g., team evaluations, improvement meetings and feedback from the audited department. However, since organizations are constantly exposed to new risks due to rapid changes in the business environment, and the need for adaption to these changes is growing (Betti and Sarens, 2020), the necessity of continuous improvement is highlighted. Furthermore, with consideration to the new and upcoming internal auditors at the STA, it could be beneficial to further elaborate on the continuous improvement work to include additional perspectives and

shared experiences. By applying the PDSA cycle, explained by Gremyr et al. (2020), to the internal audit process, continuous improvements can be incorporated. Literature regarding continuous improvement emphasize the crucial need for documentation of new and improved ways of working. Furthermore, the PDSA cycle is iterative and can be tested in a small scale, which enables recognition if changes were appropriate or not. Additionally, the PDSA cycle can facilitate a more effective internal audit process according to Nichols (2014), and also in achieving a more systematic approach for continuous improvement, while avoiding high cost on investment (Gremyr et al., 2020). Since results in Table 4.1 are showing that e.g., the supplementary risk analysis lacks documented instructions, it could be appropriate to test new methods on a small scale by applying the PDSA cycle into the audit engagement process as illustrated in Figure 5.1. This can contribute to the continuous improvement work within the internal audit function at the STA and also a more systematic approach of the current process.

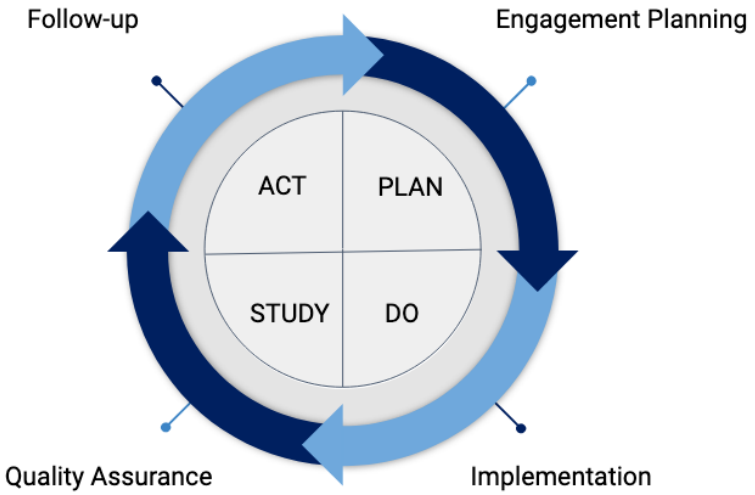

Figure 5.1: PDSA cycle applied to an internal audit engagement and its process.

As previously mentioned, there are several initiatives for improving the internal audit function at the STA and its associated process, however, our perception is that changes are of a slower and modest character. Since the STA is driven by the state, the organization might undertake a more cautious approach on changes, since it may require a more careful treatment due to its status in the society. Therefore, using a rapid and flexible approach like the PDSA cycle might be suitable for the STA, allowing for actual testing of new and improved methods.

5.2 Risk Management in Internal Audit Practices

RQ 2: *How can an internal audit function strengthen risk management in engagement planning?*

The evolution of internal audit engagements mirrors the changes made in the business environment. Coetzee & Lubbe (2014) highlights this evolution and suggest that the internal audit practices are not static but rather adaptive to the business environment. This adaptability is important for internal auditing to remain effective in identifying and

managing new risks. Moreover, recent global events such as the financial crisis and the COVID-19 have further emphasized the need for internal auditing to continue to adapt. Therefore, in the context of the STA, remaining updated on risk management in relation to changes in the business landscape is important. While findings show that the STA employ surveillance areas to monitor risks, it is important that these areas is comprehensive. However, given the size of the STA and the relatively small internal audit function, it may be difficult to identify all emerging risks. Thus, it is important that the STA has high level of risk maturity throughout the organization, where risks are managed and controlled in a reliable way enabling internal auditors to focus on their responsibilities. Furthermore, it becomes vital to allocate risk responsibilities across the three lines of defense to prevent internal auditors from undertaking duties of the second or first line. However, in organization with low-risk maturity, literature highlights that it is important for internal auditing to perform their own risk assessment to maintain objectivity and independence (Coetzee & Lubbe, 2014), which is also shared by respondent X.

The importance of engagement planning is widely acknowledged in literature (Arwinge, 2016; Rife, 2006). Rife (2006) highlights that planning is crucial for a successful audit, and that inadequate planning may entail the need for adjustment of scope and objectives later in the audit process. This view is also reflected by internal auditors at the STA and respondent X. Several internal auditors at the STA stressed that planning is vital for establishing a clear scope and objectives of the audit. However, internal auditors at the STA also addressed that planning is challenging and requires careful consideration and flexibility, highlighting the need to remain adaptive to unexpected changes that might occur. Another aspect of engagement planning that was brought up by several internal auditors of the STA was that individual opinions are incorporated into parts of the engagement planning, which highlight the subjective nature of planning. A supplementary risk assessment can be utilized in engagement planning to facilitate the establishment of significant risks, and clear scope and objectives for the audit engagement.

According to Pungas (2003) an essential part of internal auditing is to perform a risk assessment to understand the nature of risks and how to manage them effectively. Furthermore, Coetzee and Lubbe (2014) stresses the importance of understanding risks and how they change over time. Pungas (2003) further elaborates the importance of additional aspects, that might not be considered in a risk assessment, such as existing activity plans and information from former audits. This is also brought up by several respondents, highlighting the importance of performing a risk assessment to understand the current status of risks and the relevance of the audited area. Respondent X also shares this view, and points out that it is important to understand if any changes has occurred since the initial risk assessment.

The internal auditing documentation at the STA explains the risk analysis approach, where inherent risks are considered in the establishment of the annual audit plan and where residual risks are processed in the engagement planning. This approach is in line with literature, highlighting the risks assessment at both micro and macro level (Allegrini & D'Onza, 2003; Ramamoorti et al., 1999). Furthermore, micro assessment focuses on the specific audit engagement, facilitating orientation and scope of the audit

engagement. It is perceived that internal auditors at the STA updates the risk profile in the engagement planning. However, there does not seem to be a structured approach for this activity. Internal auditors at the STA with longer work experience seemed to be more comfortable with the unstructured process, while others preferred a more structured process to feel more comfortable, and to ensure that nothing is missed. In the context of the STA, several internal auditors stated that their internal auditing practices are risk-based. This is also emphasized by Coetzee and Lubbe (2014), arguing for a broader application of risk-based internal auditing which extends beyond the annual audit plan to the specific audit engagements, implying that the risk-based internal auditing needs to be incorporated throughout the processes. However, several respondents at the STA mention the need for a more systematic approach, e.g., in the supplementary risk analysis in the engagement planning, which could benefit the risk-driven approach.

Several authors stress the importance of conducting a risk assessment at a micro level, in each audit engagement, to support the risk-driven approach of internal auditing (Allegrini & D'Onza, 2003; Coetzee & Lubbe, 2014; Ramamoorti et al., 1999). However, both literature and the findings of this report implies that engagement planning is an important step to determine clear objectives and scope for the audit engagement (Arwinge, 2016). Therefore, the researchers believe it would be beneficial to conduct a risk assessment in the engagement planning, to avoid rework later in the audit engagement. To our knowledge, the risk assessment methods explained in theory are seldom explained in the context of engagement planning. However, McNamee (1996, as cited in Ramamoorti et al. 1999) defines a risk assessment process for audit engagements, explained in three steps, including identification of risks, measuring of risks and prioritization of risks. To support the risk driven approach, an extension of the risk assessment process defined by McNamee (1996, as cited in Ramamoorti et al. 1999), has been developed, illustrated in Figure 5.2. The model is based on risk management theory in connection to findings of the research. Moreover, our analysis resulted in two additional steps for the model, i.e., Evaluate and Align. The model is designed to create a structure and a descriptive approach for managing risks, while remaining simple and easy to use, with consideration for avoidance of additional and unnecessary work.

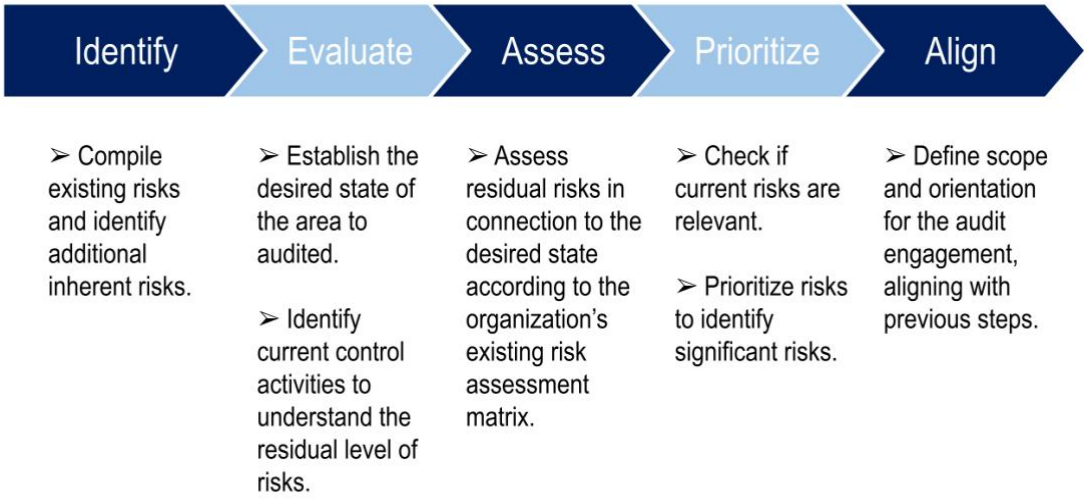

Figure 5.2: An extended risk assessment model for managing risks in the engagement planning to facilitate in defining audit engagements.

5.3 Knowledge Management

RQ 3: *How can an internal audit function adopt knowledge management practices to improve audit engagements?*

KM is key to develop and maintain organizational knowledge for new value-creation, providing competitive advantage (Hock-Doepgen et al., 2021). In the internal audit function of the STA, a need for more standardized processes has been identified, requiring a shift from reliance of "know-how" and individual expertise to organizational knowledge. This shift occurred when new team members joined, having different experiences and perspectives. It was revealed that documentation is not consistently describing processes in detail. Instead, documentation tend to focus on the result, and what to achieve, leading to ambiguity on how to perform certain activities. A way towards standardization is through transforming individual knowledge into organizational knowledge, and documenting best practices (North & Kumta, 2018).

To adopt KM theory in an internal audit function, an understanding of what knowledge is tacit or explicit can be useful in order to utilize knowledge possessed by the organization. Findings show that a lot of valuable knowledge is tacit and remains unseen, such as skills related to risk assessment, which is partially intuitive. Furthermore, internal auditors relying on their gut-feeling and experience underscores that tacit knowledge is used in their current practices. For example, respondent A noted the role of intuition to guide risk assessments, while respondent B explained that some activities are dependent on internal auditors and their individual knowledge, rather than common ways of working. This implies a reliance of tacit knowledge possessed by the internal auditors. KM is about leveraging tacit knowledge, and in order to utilize this form of knowledge, internal auditors need to use methods for transforming tacit knowledge into explicit knowledge, as suggested by literature (North & Kumta, 2018). As mentioned by Nonaka and Takeuchi (1995), the SECI model is used to describe ways of transforming knowledge. One way of transforming knowledge is by socialization, which involves the sharing of tacit knowledge between individuals,

mainly through social interactions (North & Kumta, 2018). The findings show that socialization is quite evident in the way that experienced internal auditors pass on their knowledge to newer recruits, especially when working in audit teams. By working in audit teams, the internal auditors can share their experience, and the newly recruited can observe and imitate the senior internal auditor and vice-versa. Socialization also occurs during planning meetings where internal auditors can collaborate and contribute with their expertise to help in planning the audit. To increase the level of socialization it is important to encourage a culture of knowledge sharing and collaboration (Easa, 2012), which is displayed by internal auditors at the STA. There are several examples of internal auditors at the STA, using externalization to transform tacit knowledge into explicit concepts that can be shared and communicated easily (North & Kumta, 2018). For example, in the feedback process where internal auditors conduct targeted interviews and collect implicit knowledge and insights from managers which may be converted into explicit feedback, which can be used to improve the processes within internal auditing. An additional example is during the planning meetings, where all internal auditors is invited to contribute with their expertise and to share their implicit knowledge regarding e.g., scope and limitations. This implicit knowledge can be used when producing their audit reports, since the knowledge is documented.

Combination is exemplified by internal auditors when planning an engagement, especially when developing an understanding of the context of the area to be audited. During this process, the internal auditors synthesize diverse sources of information, such as past performed audits or learning about new emerging risks. All of these sources are explicit and by synthesizing this knowledge, new insights can be created (North & Kumta, 2018). Furthermore, the internal audit function has established documented procedures and practices, which enables explicit knowledge to be transformed into tacit knowledge through practical experience, which is a form of internalization. For example, during audit engagements, internal auditors can apply explicit knowledge in practice throughout various phases of the audit engagement process such as planning, implementation, quality assurance, and follow-up. Through these hands-on experiences, internal auditors can internalize knowledge and develop tacit knowledge. However, to achieve higher levels of internalization, internal auditors may further refine their documentation of processes to serve as an even better reference for internal auditors on how to perform specific activities (North & Kumta, 2018).

KM can be utilized to leverage the existing knowledge within an internal audit function, and to transform individual knowledge into organizational knowledge (Hock-Doepgen et al., 2021). By applying the theory of KM, the SECI model has been used and incorporated into the internal auditing process, as shown in Figure 5.3. Activities of the internal audit process has been divided into the different categories of the SECI model to illustrate how knowledge may be shared, transformed and developed within the internal auditing process.

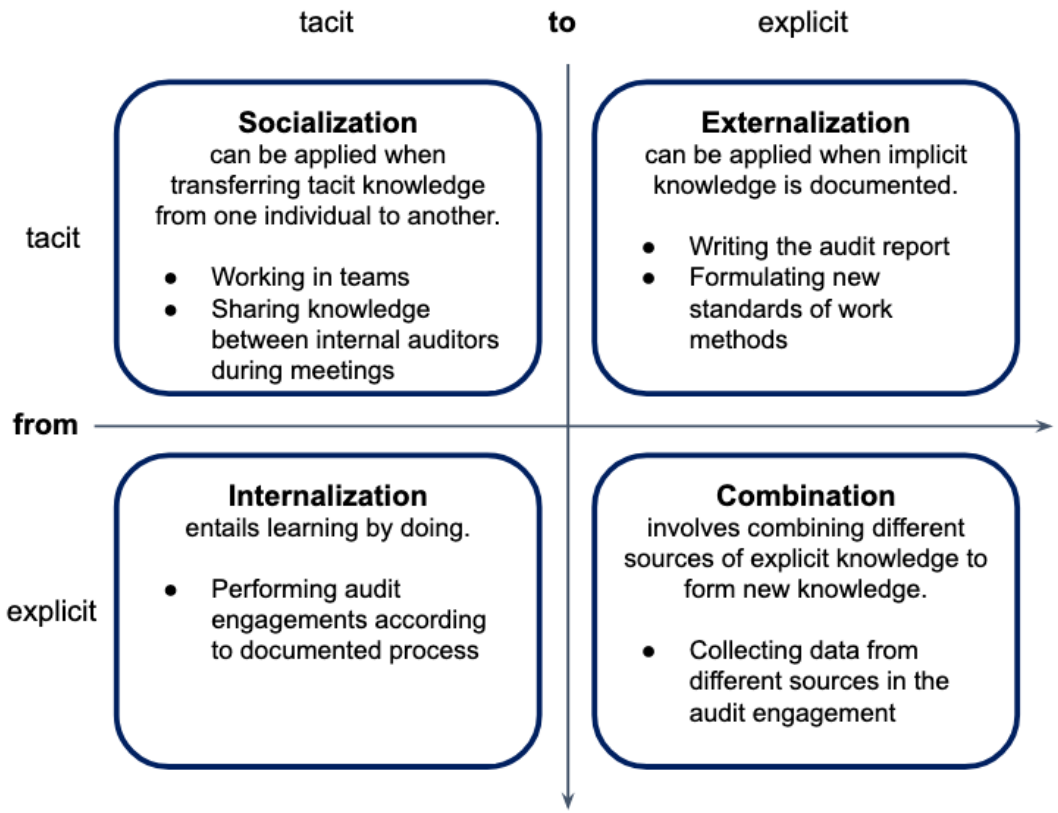

Figure 5.3: SECI model applied to an internal audit process, categorizing activities performed by internal auditors.

6. Conclusion

The purpose of this research was to explore improvements for performing internal audit processes, using risk- and KM theories. Furthermore, this thesis aimed to present an applicable model for risk assessment within engagement planning.

RQ 1: *How does an internal audit function perform an audit in practice, and how is the audit process described in documentation?*

The documented process consists of a structured and comprehensive description on how to conduct an internal audit, including the process steps and associated activities. However, some activities performed by the internal auditors are not documented and does not have a standardized way for conducting specific activities, as shown in Table 4.1. Consequently, internal auditors perform these activities individually, without clear instructive references in documentation.

RQ 2: *How can an internal audit function strengthen risk management in engagement planning?*

To maintain the risk-driven approach of the internal audit engagements, continuous improvement of risk management throughout the audit engagement becomes essential. Establishing a way for conducting risk assessment at a micro level in the engagement planning phase can facilitate in finding significant risks, and also defining scope and orientation for the audit engagement. Furthermore, a risk assessment in the engagement planning should be based on residual risks and consider aspects beyond the risk assessment in the annual audit plan as explained in Figure 5.2. Aspects to consider include e.g., identification of new risks, finding out if the risk is still relevant, investigate if there are any existing activity plans and deciding if the audit engagement is perceived as value-adding.

RQ 3: *How can an internal audit function adopt knowledge management practices to improve audit engagements?*

The role of internal auditors is knowledge intensive, inhibiting a lot of valuable tacit knowledge, which is mostly intuitive and experience based. KM practices can improve audit engagements by applying the SECI model, as shown in Figure 5.3, by e.g., transforming individual knowledge into organizational knowledge through formulating new standards of work methods. Furthermore, the model enables knowledge to be shared and developed, since tacit knowledge may be made into explicit knowledge. Hence, facilitating more standardized processes, which in turn can contribute to improved audit engagement.

6.1 Recommendations

To address improvement areas, and processes that may lack instructive documentation, recommendations for the internal audit function at the STA has been developed. By incorporating both risk- and KM practices, the internal audit function

can improve its current process. Recommendations for the internal audit function include:

- As a group, reflect upon a reasonable level of instructive descriptions for activities identified in Table 4.1 to achieve consistent results of audit engagements. Take advantage of the SECI model to share knowledge and individual ways of working to find a common way of working, forming a best practice.

- Implementing PDSA cycle into the audit engagements, according to Figure 5.1, to continuously improve the process. In each specific audit engagement, new changes can be tested and implemented at a small scale by using the PDSA cycle. Changes contributing to an improved process can be implemented and further developed in the upcoming cycle, while unsuccessful changes can be rejected.

- Implementing the extended risk assessment model presented in Figure 5.2 to add structure for managing risks in the engagement planning to facilitate in defining audit engagements. Furthermore, adapt the model to the planning phase of the internal audit process and use the PDSA cycle to continuously revise and improve the model.

6.2 Theoretical Implications

Quality research has focused on external auditing rather than internal auditing, and this study expands on the internal auditing role within quality management in literature. Findings suggest that internal auditing requires standardized ways of working that is flexible in its nature to adapt to changes in the business environment. A comparison between the documented instructions and activities performed in practice has been conducted in the research, which to our knowledge has not previously been done in academic literature. Furthermore, findings suggest that a supplementary risk analysis can aid in defining audit objectives, scope, and limitations in the planning phase of an audit engagement to achieve an effective audit. Additionally, in a supplementary risk analysis it's vital to establish the desire state in relation to the audit objectives, scope, and limitations. Therefore, this research adds on to existing risk management theories by developing a model for risk assessment in engagement planning. Specifically, the proposed model adds on to existing risk assessment process defined by McNamee (1996) with two additional steps, including Evaluate and Align. The model can be applied to internal auditing processes with a similar setting as the case study. It may be more useful within large organizations that are exposed to a great number of risks that need to be effectively managed. Moreover, findings show that internal auditors inhibit a high level of tacit knowledge in relation to engagement planning. Aiming to facilitate the use of existing knowledge, this research has applied the SECI model in the context of internal audit engagements and associated process activities, which is a theoretical contribution to existing KM theory. The model can be incorporated into firms performing internal audits and can also serve as an example for internal audit functions to develop activities that enhance knowledge management practices.

6.3 Limitations

This master's thesis has been limited to a single case study at a public and large organization in Sweden. Therefore, the results might not be generalizable and perhaps not applicable in other business constellations or contexts. However, a thick description of the case was given to aid in generalizability. Moreover, the sample size was relatively small, which was partially due to the few employees within the internal audit function at the STA. Given that the data, to a high extent, consists of interviews, it might imply that some information might be missed. The limitations points to future research topics, addressed in the subsection below.

6.3.1 Future Research

For future research, exploring other contexts by e.g., conducting the research in another continent or in a private organization would be interesting. Additionally, a study consisting of several case studies would achieve findings that may be more generalizable. The proposed risk assessment model for the STA is not specifically developed for the organization, aiming to be general and applicable for all types of organizations with similar structure as the case study. However, this model has not been tested, which could be evaluated in future research. Furthermore, this study implies that KM practice can be adopted to achieve effective audit engagements, however, future research could explore the effects of incorporating KM into internal auditing.

References

Adams, J. (2007). *Research methods for graduate business and social science students*. SAGE Publications.

Albawwat, I. E. (2022). Tacit knowledge sharing in small audit firms and audit quality inputs: The antecedent effect of auditors' social capital. *Journal of Knowledge Management*, *26*(9), 2333–2353. https://doi.org/10.1108/JKM-02-2021-0113

Allegrini, M., & D'Onza, G. (2003). Internal Auditing and Risk Assessment in Large Italian Companies: An Empirical Survey. *International Journal of Auditing*, *7*(3), 191–208. https://doi.org/10.1046/j.1099-1123.2003.00070.x

Anugraheni, E. P., Setiawati, E., & Trisnawati, R. (2022). Analysis of Risk-Based Internal Audit Planning Implementation and Its Impact on Audit Quality: Case Study at the Inspectorate of Surakarta, Indonesia. *Journal of Economics and Business*, *5*(3). https://doi.org/10.31014/aior.1992.05.03.448

Arwinge, O. (2016). *Internrevision—En introduktion*. Sanoma Utbildning.

Bell, E., Bryman, A., Harley, B., & Bryman, A. (2019). *Business research methods.* (Fifth edition). Oxford University Press.

Betti, N., & Sarens, G. (2020). Understanding the internal audit function in a digitalised business environment. *Journal of Accounting & Organizational Change*, *17*(2), 197–216. https://doi.org/10.1108/JAOC-11-2019-0114

Coetzee, P., & Lubbe, D. (2014). Improving the Efficiency and Effectiveness of Risk-Based Internal Audit Engagements. *International Journal of Auditing*, *18*(2), 115–125. https://doi.org/10.1111/ijau.12016

Cordeiro, E., Lermen, F. H., Mello, C. M., Ferraris, A., & Valaskova, K. (2024). Knowledge management in small and medium enterprises: A systematic literature review, bibliometric analysis, and research agenda. *Journal of Knowledge Management*, *28*(2), 590–612. https://doi.org/10.1108/JKM-10-2022-0800

COSO. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance*. https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

COSO. (2023). *Achieving Effective Internal Control over Sustainability Reporting (ICSR): Building Trust and Confidence through the COSO Internal Control—Integrated Framework*. https://www.coso.org/_files/ugd/3059fc_a3a66be7a48c47e1a285cef0b1f64c92.pdf

Duh, R.-R., Knechel, W. R., & Lin, C.-C. (2020). The Effects of Audit Firms' Knowledge Sharing on Audit Quality and Efficiency. *Auditing: A Journal of Practice & Theory*, *39*(2), 51–79. Business Source Ultimate. https://doi.org/10.2308/ajpt-52597

Easa, N. F. (2012). *Knowledge management and the SECI model: A study of innovation in the Egyptian banking sector*.

Fox, C. (2018). Understanding the new ISO and COSO updates. *Risk Management*, *65*(6), 4–7.

Gasparotti, R. F., & Gasparotti, C. M. (2023). Impact of internal audit activity on risk management within construction organization. *Romanian Association of Managers and Economic Engineers from Romania*, *22*(3), 189–208.

Gremyr, I., Bergquist, B., & Elg, M. (2020). *Quality Management—An Introduction*. Studentlitteratur AB.

Gyllenhammar, D., & Hammersberg, P. (2023). How to facilitate improvements in public service systems: Propositions for action. *International Journal of Quality & Reliability Management*, *40*(6), 1429–1448. https://doi.org/10.1108/IJQRM-09-2021-0314

Hock-Doepgen, M., Clauss, T., Kraus, S., & Cheng, C.-F. (2021). Knowledge management capabilities and organizational risk-taking for business model

innovation in SMEs. *Journal of Business Research*, *130*, 683–697. https://doi.org/10.1016/j.jbusres.2019.12.001

Hopkin, P. (2017). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (Fourth edition). Kogan Page.

Hutchinson, B., Dekker, S., & Rae, A. (2024). Audit masquerade: How audits provide comfort rather than treatment for serious safety problems. *Safety Science*, *169*, 106348. https://doi.org/10.1016/j.ssci.2023.106348

International Organization for Standardization. (2018a). *Guidelines for auditing management systems (ISO 19011:2018)*. https://www.iso.org/standard/70017.html

International Organization for Standardization. (2018b). *Risk management—Guidelines (ISO 31000:2018)*. https://www.iso.org/standard/65694.html

Khairunnisa, L. (2020). Role of the Internal Auditors in Improving the Quality Management System Integrated ISO 9001: 2015 and 22716: 2007. *Journal of Research in Business, Economics, and Education*, *2*(4), 784–798.

Kim, D.-Y., Kumar, V., & Kumar, U. (2012). Relationship between quality management practices and innovation. *Journal of Operations Management*, *30*(4), 295–315.

Kotb, A., Elbardan, H., & Halabi, H. (2020). Mapping of internal audit research: A post-Enron structured literature review. *Accounting, Auditing & Accountability Journal*, *33*(8), 1969–1996. https://doi.org/10.1108/AAAJ-07-2018-3581

Krstić, J., & Dordević, M. (2012). Internal control and enterprise risk management—From tradicional to revised COSO model. *Economic Themes*, *50*(2), 151–166.

Kuei, C., & Lu, M. H. (2013). Integrating quality management principles into sustainability management. *Total Quality Management & Business Excellence*, *24*(1–2), 62–78. https://doi.org/10.1080/14783363.2012.669536

Kuei, C.-H., Madu, C. N., & Lin, C. (2008). Implementing supply chain quality

management. *Total Quality Management & Business Excellence*, *19*(11), 1127–1141. https://doi.org/10.1080/14783360802323511

Lazarus, S., Lazarus, R., & Rajendran, A. (2021). The roles, challenges and benefits of internal auditing in organizations. *International Journal of Accounting & Finance Review, 7*(1), 103–122.

Lenz, R., & Hahn, U. (2015). A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal*, *30*(1), 5–33. https://doi.org/10.1108/MAJ-08-2014-1072

Mai, D. N., & Nguyen, H. T. L. (2022). A Knowledge Management Model for Internal Auditing. *European Conference on Knowledge Management*, *2*, 768-776,R33.

Manos, A. (2007). The benefits of Kaizen and Kaizen events. *Quality Progress*, *40*(2), 47.

Mehmeti, F. (2018). Common Characteristics and Differences in External and Internal Auditing. *European Journal of Economics and Business Studies, 4*, 261–267. https://doi.org/10.2478/ejes-2018-0030

Moeller, R. R. (2011). *COSO enterprise risk management: Establishing effective governance, risk, and compliance processes* (2nd ed). Wiley.

Moen, R., & Norman, C. (2006). *Evolution of the PDCA cycle*.

Morrow, P. C. (1997). The measurement of TQM principles and work-related outcomes. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, *18*(4), 363–376.

Nguyen, L., & Kohda, Y. (2017). Toward a Knowledge Management Framework for Auditing Processes: *International Journal of Knowledge and Systems Science*, *8*(3), 45–67. https://doi.org/10.4018/IJKSS.2017070104

Nichols, A. (2014). *A Guide to Effective Internal Management System Audits: Implementing internal audits as a risk management tool*. IT Governance Publishing.

Nissinboim, N., & Naveh, E. (2018). Process standardization and error reduction: A revisit from a choice approach. *Safety Science, 103*, 43–50.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

North, K., & Kumta, G. (2018). *Knowledge Management: Value Creation Through Organizational Learning* (2nd ed. 2018). Springer International Publishing : Imprint: Springer. https://doi.org/10.1007/978-3-319-59978-6

Prawitt, D. F. (2003). Managing the internal audit function. In *Research opportunities in internal auditing*. Institute of Internal Auditors Research Foundation.

Pungas, K. (2003). Risk Assessment as Part of Internal Auditing in the Government Institutions of the Estonian Republic. *EBS REVIEW*, 42–46.

PwC. (2015). *2015 State of the Internal Audit Profession Study: Finding True North in a period of rapid transformation*. https://www.pwc.com/ve/es/auditoria-interna/assets/pwcs-2015-state-of-the-internal-audit-profession-study.pdf

Raiborn, C., Butler, J. B., Martin, K., & Pizzini, M. (2017). The Internal Audit Function: A Prerequisite for Good Governance. *Journal of Corporate Accounting & Finance*, *28*(2), 10–21. https://doi.org/10.1002/jcaf.22246

Ramamoorti, S., Bailey Jr, A. D., & Traver, R. O. (1999). Risk assessment in internal auditing: A neural network approach. *International Journal of Intelligent Systems in Accounting, Finance & Management*, *8*(3), 159–180. https://doi.org/10.1002/(SICI)1099-1174(199909)8:3<159::AID-ISAF169>3.0.CO;2-W

Rife, R. (2006). Planning for success: Audit effectiveness often hinges on work done prior to the engagement. *Internal Auditor*, *63*(5), 25–28.

Ryan, G. W., & Bernard, H. R. (2003). Techniques to Identify Themes. *Field Methods*, *15*(1), 85–109. https://doi.org/10.1177/1525822X02239569

Samagaio, A., & Felício, T. (2023). The determinants of internal audit quality. *European Journal of Management and Business Economics*, *32*(4), 417–435.

https://doi.org/10.1108/EJMBE-06-2022-0193

Sanchez, L., & Blanco, B. (2014). Three decades of continuous improvement. *Total Quality Management & Business Excellence*, *25*(9–10), 986–1001.

Simon, A., Yaya, L. H. P., Karapetrovic, S., & Casadesús, M. (2014). An empirical analysis of the integration of internal and external management system audits. *Journal of Cleaner Production*, *66*, 499–506. https://doi.org/10.1016/j.jclepro.2013.11.020

Swedish Transport Administration. (2021). *Styrelsens riktlinjer för Internrevisionen* [Unpublished internal company document].

Swedish Transport Administration. (2023). *Internrevisionens revisionsplan 2024-2026* [Unpublished internal company document].

Swedish Transport Administration. (2024a). *Internrevisionshandboken* [Unpublished internal company document].

Swedish Transport Administration. (2024b). *Vår organisation*. https://www.trafikverket.se/om-oss/var-verksamhet-vision-och-uppdrag/organisation/

Szabo, A. (2012). Risk management: An integrated approach to risk management and assessment. *University of Oradea*.

The Institute of Internal Auditors. (2017). *International Professional Practices Framework (IPPF)* (2017 edition). The Institute of Internal Auditors.

The Institute of Internal Auditors. (2020). *THE IIA'S THREE LINES MODEL*. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

The Institute of Internal Auditors. (2024). *About Internal Audit.* https://www.theiia.org/en/about-us/about-internal-audit/

Ungan, M. C. (2006). Standardization through process documentation. *Business Process Management Journal, 12*(2), 135–148.

Wang, X., Ferreira, F. A., & Yan, P. (2023). A multi-objective optimization approach for integrated risk-based internal audit planning. *Annals of Operations Research*, 1–30.

A. Interview Guide

A.1: Semi-structured Interview at the STA

Audit Projects

- What activities do you carry out during the planning phase?
- In what order do you typically perform the various activities in the planning phase, and is there a reason for conducting the steps in this order?
- What information do you bring into the planning phase from the annual audit plan, including any prepared materials?
- Do you conduct an in-depth risk analysis for individual audit objects, and if yes, how do you approach it to ensure the audit remains relevant?
- How would you explain the approach in the planning phase to a newly hired employee?

Internal Planning Meeting

- Who participates in this meeting?
- Can you describe such a meeting, including details about the agenda, open discussion, brainstorming, structure, and what is presented?
- What is the typical outcome of an internal planning meeting?
- In brainstorming sessions, what is the result, and how is it utilized? (E.g., is it for inspiration for the audit team, or is there a systematic way to "sort" thoughts and ideas? Do you include everything or select ideas that the group agrees are suitable?)

External Planning Meeting

- Who participates?
- Can you describe such a meeting, including details about the agenda, open discussion, brainstorming, structure, and what is presented?
- What is the typical outcome of an external planning meeting?

Focus and Scope of Audit Objects

- How do you usually define a purpose for your project?

- How do you determine a reasonable focus for an audit object in the planning phase, including any key activities, factors considered, and methods used?

- How do you limit the scope of an audit object, including any key activities, factors considered, and methods used?

- Have there been any previous instances where the purpose of an audit object was unclear, and how could it be improved?

Concluding questions

- What do you consider central in the planning phase?

- If you were to structure the planning phase using a checklist based on your experience, what specific points would you include?

- What characterizes a well-executed audit for you, and how do you confirm it?

- What is your goal with an audit, and what do you aim to achieve with it?

- How do you work to develop your audit work, and if so, how?

- How do you work on continuous improvement of the process?

- Are there occasions when the audited entity (or the board) provides feedback on your work, and how is that feedback used in future audits?

A.2: Semi-structured Interview with Expert

- Tell me more about yourself? Who are you? (What is your role? Background?)

- Can you tell me about your organization?

- Can you provide an insight into the International Professional Practices Framework? How does this framework support different auditors? What are the fundamental standards?

- How are different audit projects planned?

- How do you determine the scope and focus of various audit projects?

- How is the annual risk analysis conducted?

- How are the risks prioritized?

- Is there any built-in improvement work?
- How do you work on continuous improvement of the internal audit process? Are there different milestones?
- What characterizes a well-conducted audit?
- What do you think the future holds for the profession?

DEPARTMENT OF TECHNOLOGY MANAGEMENT AND ECONOMICS
DIVISION OF INNOVATION AND R&D MANAGEMENT
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden
www.chalmers.se

CHALMERS
UNIVERSITY OF TECHNOLOGY