UNIVERSITY OF TURKU

Enhancing Cybersecurity Compliance in Finnish SMEs: Evaluation and Adoption of Scalable GRC Tools

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Manish Das

Supervisors:

M.Sc. Saku Lindroos

D.Sc. Antti Hakkala

December 2025

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Manish Das
Title: Enhancing Cybersecurity Compliance in Finnish SMEs: Evaluation and Adoption of Scalable GRC Tools
Number of pages: 50 pages, 5 appendix pages
Date: December 2025

Abstract.

The evolving cybersecurity regulatory landscape pose a significant challenge for Small and Medium-sized Enterprises (SMEs), which often lack the financial resources, in-house expertise, and time to achieve compliance efficiently. This thesis investigates the potential of Governance, Risk, and Compliance (GRC) tools as a solution, focusing specifically on their scalability and adoption within the Finnish SME context.

The study includes review of related scientific literatures, comprehensive survey of Finnish SMEs and comparative analysis of four GRC solutions. The literature review established a foundation for analysing cybersecurity compliance practices and adoption of GRC tools by SMEs. The survey served to quantify the compliance challenges, tool preferences and adoption barriers for the SMEs in Finland. The strategically chosen open source to commercial and global to regionally focused tools were evaluated against a framework of economic, operational, technical and viable scalability criteria.

The findings reveal a critical scalability gap in the GRC tool market. Finnish SMEs are predominantly challenged by cost, staff time, expertise and framework complexity constraints leading to reliance on manual and ad-hoc methods for compliance. The analysis demonstrates that available tools force a trade-off between economically and operationally scalable options.

The thesis provides tripartite recommendations suggesting SMEs to adopt a strategic tool selection approach, GRC vendors to develop lightweight SME focused solutions and policymakers to enhance outreach efforts and provide simplified implementation guidance. This study concludes that bridging the identified scalability gap requires a coordinated effort from all stakeholders to ensure GRC solutions are effective and accessible for Finnish SMEs.

Keywords: GRC tools, Compliance, Finnish SMEs, Cybersecurity.

Table of contents

Abbreviations

SMEs – Small and Medium Enterprises

GRC – Governance, Risk and Compliance

GDP – Gross Domestic Product

PCI DSS – Payment Card Industries Data Security Standard

HIPAA – Health Insurance Portability and Accountability Act

ISMS – Information Security Management Systems

NCC – National Coordination Centre

NCSC-FI – National Coordination Centre of Traficom's Finnish Cybersecurity Centre

ENISA – European Union agency for Cybersecurity

GDPR – General Data Protection Regulation

COBIT – Control Objectives for Information and Related Technologies

ISO/IEC – International Organisation for Standardisation and International Electrotechnical Commission

NIS2 – Network and Information Systems Directive 2

CIS controls – Centre for Internet Security Controls

PDCA – Plan-Do-Check-Act

CSIRT – Computer Security Incident Response Team

EU-CyCLONe – European Cyber Crisis Liasion Organization Network

ISACA – Information System Audit and Control Association

C2M2 – Cybersecurtiy Capability Maturity Model

SWOT – Strength Weakness Opportunities Threat

CIA – Confidentiality Integrity Availability

IGA – Identity Governance and Administration

CYSEC – Cybersecurity Coach

SaaS – Software as a Service

AI – Artificial Intelligence

1 Introduction

Cybersecurity has become a crucial requirement for organizations of all sizes. The increasing use of digital services, regulatory obligations, and the growing sophistication of cyber threats demand robust and structured efforts to protect businesses. Small and medium-sized enterprises (SMEs), which make 54.1% of the total turnover from companies in Finland and 40% of the national Gross Domestic Product (GDP), are particularly vulnerable to cyber threats [1]. However, their limited financial and human resources often restrict the ability to establish robust Governance, Risk management, and Compliance (GRC) practices. As a result, SMEs face risks of data breaches, regulatory penalties, and reputational damage. There are limited studies that illustrates the state of cybersecurity compliance by SMEs in Finland. However, bodies like National Coordination Centre of Traficom's Finnish Cybersecurity Centre (NCC-FI) provide financial support to help SMEs to build or improve their cybersecurity posture.

The regulatory environment for cybersecurity compliance has become increasingly complex in Finland. Frameworks such as International Organisation for Standardisation and International Electrotechnical Commission (ISO/IEC) 27001, the General Data Protection Regulation (GDPR), and the European Union's (EU) new Network and Information Systems Directive (NIS2) Directive impose significant governance and reporting obligations on organisations. At the same time, practical tools and support structures exist to assist SMEs, including EU and European Union Agency for Cybersecurity (ENISA) initiatives such as SecureSME which has been discontinued now and the current 12 steps guidelines to securing businesses. However, adoption remains uneven, and many SMEs continue to struggle with aligning compliance requirements to their day-to-day business operations.

Without accessible and scalable solutions, SMEs risk remaining underprepared for cybersecurity incidents, thereby threatening their resilience and competitiveness in the European digital economy. Despite the availability of established frameworks and GRC tools, SMEs in Finland face persistent challenges in achieving effective cybersecurity compliance. These challenges include:

1. Limited resources and expertise to interpret and implement compliance requirements [2].
2. Perceived complexity and cost of existing frameworks such as ISO 27001 [3].
3. Lack of SME-specific usability in many GRC tools [3].

4. External pressures from supply chain requirements and new regulatory obligations (e.g., NIS2) [4].

1.1 Research Gaps

Although there have been a significant number of studies in cybersecurity frameworks and GRC tools functions, the reviewed literatures in this thesis identify some of the gaps on how the implementation of GRC tools can actually enhance cybersecurity compliance in SMEs while leading to smooth scalability across different sectors especially in Finland. The regulatory and technical dimensions of cybersecurity compliance are well-documented, however, there is limited empirical research examining how SMEs operationalise compliance through GRC systems. In case of Finland, the studies are insufficient regarding scalable compliance management in SMEs. It was found that the adoption of GRC primarily on large enterprises where structured governance models, dedicated teams and significant financial resources are adequate. This leads to incompatible design of existing solutions for SMEs which are generally resource and finance constrained.

The cybersecurity standards and frameworks such as ISO 27001, NIST CSF and NIS2 directive provide structured approaches for managing information security and legal obligations. However, there is a gap on how SMEs can operationalise security practices specific to their risk environment to meet those high-level regulatory requirements. This thesis aims to address this gap by investigating the relation between compliance requirements, organisational capability, GRC tools usability and factors affecting adoption in Finnish SMEs. This will provide a foundation to develop and implement a scalable GRC solution for tool vendors, policymakers and the SMEs in Finland.

1.2 Research Aim and Objectives

The overall aim of this thesis is to evaluate how scalable GRC tools can enhance cybersecurity compliance in Finnish SMEs. Specifically, the objectives are to:

1. Analyse the main challenges Finnish SMEs face in achieving cybersecurity compliance.
2. Review existing compliance frameworks (ISO 27001, NIS2, COBIT, NIST CSF, CIS controls, Kybermittari (Cybermeter)) and their relevance for SMEs.
3. Evaluate the usability and effectiveness of selected GRC tools for SMEs.

4. Identify the key factors influencing adoption and non-adoption of GRC tools.
5. Provide recommendations for improving cybersecurity compliance through scalable, user-friendly solutions in Finnish SMEs.

1.3 Research Questions

The following research questions are proposed to guide and structure this thesis. These questions are aimed to establish a research framework that balances theoretical review with practical inquiry to ensure that the study incorporates both the systemic challenges and the real experiences of SMEs in Finland.

1. What are the primary challenges that SMEs in Finland face in achieving cybersecurity compliance?
2. What frameworks and tools currently support SME GRC efforts?
3. How effective and usable are these tools in real-world SME environments?
4. What factors influence the adoption (or resistance to adoption) of GRC tools among SMEs?

1.4 Scope and Limitations

This thesis focuses on the SMEs in Finland across different sectors, particularly on organizations that process personal data, provide digital services or operate in critical supply chains affected by the NIS2 directive. The scope includes regulatory and industry frameworks relevant to the context of EU. The sector specific standards such as Payment Card Industries Data Security Standard (PCI DSS in payment) and Health Insurance Portability and Accountability Act (HIPAA) in healthcare which are not relevant to EU are not included in this study. The research is exploratory which uses mixed method (qualitative and quantitative) approaches. The findings will represent the evaluations of specific tools and perspective of the SMEs rather than broad large-scale generalization.

2 Governance, Risk and Compliance (GRC)

GRC is an integrated framework that aligns leadership, risk management and regulatory or advisory adherence with business objectives. It is a strategic capacity that aligns IT and business operations with organisational goals while managing risk and meeting regulatory requirements effectively. Governance defines the process and policies to steer the organisation. Risk management is a day-to-day technical process to mitigate risks that could hinder achieving business objective. Compliance is process that ensures the business operations are conducted following applicable laws, regulations, standards and even internal policies. In today's time where cyber threats are more complex and the regulatory landscapes are expanding, an integrated approach of structured GRC applied holistically can add significant value along with competitive business advantage not only for large enterprises but also for small and medium sized enterprises [5].

Traditionally, GRC have been managed in organisations through an independent, manual, ad hoc approach resulting to significant challenges such as resource drain, operational inefficiency, increased risks landscape, strategic misalignment and growth barriers. However, an integrated GRC implementation approach establishes accountability, information transparency, conscious decision making, improved risk management, value-driven unified activities and smooth growth opportunities. This centralised management enables a proactive and sustainable strategies increasing operational efficiency while reducing costs. An effective GRC enables organisations to manage complexities, reduce risks, comply with regulatory obligations and enhance performance while maintaining ethical standards [6].

In addition, GRC defines mechanisms for smooth business operation enabling business continuity to meet business objectives in case of disturbances caused by errors, anomalies and threats. Implementing effective GRC requires active commitment of top management with executional interest from all employees. Moreover, in their study Racz et al. [5] outline four basic components that are common to each domain of GRC. The components are strategy, processes, technology and people. An organisation defines strategy, policies and decision-making roles within the governance domain, inducts processes and tools in risk management and within the compliance domain, the organisation uses technologies for monitoring and relies on trained people to enforce adherence to legal and regulatory requirements. In practicality, a unified GRC approach coordinates how strategic goals are translated into operating procedures

and enforced via technology and people all while maintaining organisation's risk appetite and legal, regulatory and contractual obligations.

2.1 The pillars of GRC

2.1.1 Governance

Information sharing is a crucial for businesses regardless of organisation size in today's time. The information shared over networks benefits easy and real-time access by multiple stakeholders. This ease of access also brings management and security vulnerabilities that need policies, tools, guidelines and practices for protection and smooth operation. When there are multiple stakeholders involved, there emerge challenges of decisions-making differences, tasks duplications and inefficient practices. Governance balances the needs, conditions and options of stakeholders. It enables decision-making and prioritizing activities as well assessing them to determine common goals [7].

Governance refers to the overall system of rules, practices and standards by which an organisation is directed and controlled. It ensures the activities performed are not just technical functions but are linked to and support business objectives. Governance defines risk appetite and ensure strategic priorities. It establishes clear roles, responsibilities and accountability. It brings structure and allows management to plan, build, execute and supervise functions required to meet set objectives [7].

2.1.2 Risk management

The advancement in technology has made it easier for conducting business operations across multiple locations, domains including multiple stakeholders. The same advancement in technology has also made systems, people and infrastructures more vulnerable. The ever-evolving sophisticated threat landscape introduce several risks such as business disruptions, data leakage, reputational damage, physical damage and even organisation shutdown. Thus, robust measures are required to control and mitigate the risks in order to keep the business functions running to meet business objectives which can be achieved by a well-designed effective risk management process [8].

Risk management is a systematic process of identifying, assessing and prioritizing risks followed by allocating resources and strategies to monitor, control and mitigate the impact caused by those risks. Risk management enables identifying threats, vulnerabilities, evaluating

the likelihood of impact on business and treating the risks either to control or mitigate the impact. While risk management might be perceived as a list of problems, on the contrary, it provides insights for prioritizing actions. It provides an evidence-based foundation upon which governance decisions and compliance activities are built.

2.1.3 Compliance

There are several legal, regulations and standards established to check and balance operations of enterprises. The regulations spread across areas such as data protection, industry specific requirements, reporting and internal policies. Transparency, accountability and ethical business practices are demanded by regulators and stakeholders. Efficient and robust compliance strategies lead to adoption of this complex requirements without additional burden to organisations [9].

Compliance refers to abiding to laws, regulations, standards and internal policies that are applicable to the organisation. Compliance ensures the requirements are addressed and fulfilled. It demonstrates due diligence as it involves documentation of policies, controls, processes and evidence demonstrations to auditors, regulators and clients showcasing the organisation meets obligations. Compliance leads to development of robust programs that ensure security and business continuity. A mature compliance process protects enterprises from fines, legal costs and reputational damage.

2.2 GRC integration in SMEs

It has been established by Racz et al. [5] and Karthick et al. [6], that applying GRC framework in organisations results in effective implementation of practices, control of associated risks and adherence to regulatory obligations. Integrating GRC brings structure to operations conducted to meet set business objectives. However, applying GRC can bring its own set of challenges in SMEs that are usually resource and finance constrained. SMEs typically lack formal structures that larger enterprises have nevertheless, they face similar governance, risk and compliance challenges.

Due to resource constraints, SMEs often opt for informal GRC when tackling to threats and operational risks along with regulatory obligations. It has been noted that unstructured and inconsistent risk assessments are often applied in SMEs [8]. The ad hoc processes are implemented depending upon managerial experiences rather than having an established control

systems which increases vulnerability. Failing to prioritise compliance requirements may result in fines and loss of reputation for SMEs. Unmanaged risks can lead to loss of business, data breach and suboptimal decision making. Thus, having a structured GRC framework is important for small businesses.

Applying an integrated GRC in SMEs enables resource optimisation eliminating redundant efforts, holistic risk view with sustainable decision making and demonstrates due diligence creating audit trails of compliance activities. GRC establishes a risk appetite for organisations which helps to either accept, mitigate, avoid or transfer risks to protect business. While a comprehensive GRC programs can be unaffordable for small enterprises, they can adapt in a lightweight way to established frameworks. This means frameworks can be applied focusing on core sections of business rather than taking it to cover the whole organisation. The simplified versions of enterprise frameworks can also guide SMEs to manage and organise controls without full implementation. Additionally, use of simple toolkits and checklists for risk assessments are helpful.

Furthermore, GRC should be implemented as a part of daily operations rather than using it as a one-time activity. The results can only be valuable when it is integrated into workflows. Training and awareness about integration of GRC can boost identification of risks and treatment strategies proactively small teams of SMEs. SMEs can scale their operations securely for growth with a structured GRC program. A mature GRC program improves coordination and efficiency by reducing unnecessary practices for business operation [6].

3 Background and Theoretical Framework

This section aims to provide an overview of some widely known cybersecurity standards, frameworks and regulation. It explores the relevance of these frameworks and regulations for SMEs. The discussion reviews the role of GRC tools for cybersecurity compliance and presents an overview of the efforts implemented by regional and national bodies to support cybersecurity compliance by the SMEs in Finland. Moreover, this section underscores the importance of integrating frameworks into business practices to enhance cybersecurity posture of small and medium-sized organisations. Overall, it provides a groundwork for understanding requirements of security standards and regulatory frameworks that SMEs in Finland need to adhere and operate in.

3.1 Overview of Cybersecurity Frameworks

Cybersecurity standards are technical rules aimed to protect organization's digital environments, including users, networks, systems, processes, and data across local, cloud, and transit platforms. Cybersecurity compliance frameworks provide organizations with structured standards and best practices that guide governance, risk management, and technical implementation [10]. The frameworks are designed to help organizations identify, assess and mitigate cyber risks resulting to stronger defences and enhanced resilience. There are several cybersecurity frameworks available and recognised internationally and in EU-level. However, in this thesis, the cybersecurity frameworks that are most relevant in the context of SMEs in Finland are overviewed. Each framework or standard address different but complementary aspects of information security and regulatory compliance.

3.1.1 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 is the international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It adopts a risk-based approach and the Plan–Do–Check–Act (PDCA) cycle as core processes for continual improvement of security controls [11]. The framework requires a clearly defined ISMS scope and policy, including management commitment and documented procedures, systematic risk assessment and treatment through asset identification, risk analysis, risk matrices, and treatment plans to guide control selection and resource prioritization [12].

ISO 27002 is an application of a control catalogue. 93 controls named as Annex A controls are categorised along 4 domains; technical, organizational, people and physical, provide guidance that are tailored to manage risks, ongoing monitoring, auditing, and certification processes, including internal audits, management reviews, and external certification, to validate compliance and provide assurance [11]. Finally, a clause requiring continual improvement mechanisms where PDCA cycles, metrics, and corrective actions ensure that the ISMS evolves and strengthens over time [13].

3.1.2 NIS2 Directive (EU Directive 2022/2555)

The NIS2 Directive (EU 2022/2555) is the updated EU cybersecurity legislation that came into force in 2023, replacing the original NIS Directive of 2016. It aims to strengthen and harmonize cybersecurity resilience across member states by broadening its scope, imposing stricter obligations, and enhancing cooperation mechanisms. NIS2 expands coverage to a wider range of sectors, classifying organizations as “essential” or “important” entities depending on their role in critical infrastructure and services. It introduces comprehensive risk management obligations, including requirements for supply chain security, vulnerability handling, and secure system design. Furthermore, it enforces more rigorous incident reporting rules, obliging organizations to notify significant incidents within strict timelines [14].

Beyond risk and reporting, NIS2 establishes robust enforcement and accountability measures. National authorities are given stronger supervisory powers, while top management is made explicitly accountable for cybersecurity compliance. Member states must also implement sanctions for non-compliance and adopt coordinated crisis management strategies. To address cross-border threats, the directive enhances cooperation through national Computer Security Incident Response Team (CSIRT)s, peer reviews, and EU-level bodies like European Cyber Crisis Liasion Organization Network (EU-CyCLONe) [15]. By mandating both organizational and technical safeguards, NIS2 sets a higher, harmonized baseline of cybersecurity practices across the EU.

3.1.3 COBIT

The Control Objectives for Information and Related Technologies (COBIT) framework, developed by Information System Audit and Control Association (ISACA), is a widely adopted model for the governance and management of enterprise IT. Introduced as an IT audit tool, COBIT has since evolved into a comprehensive governance framework that aligns technology

processes with organizational strategy and compliance requirements [16]. According to ISACA, COBIT 2019, integrates principles of stakeholder value, enterprise-wide coverage, and holistic governance while maintaining compatibility with other frameworks such as ISO/IEC 27001 and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

The COBIT 2019 framework is structured into two principles; governance and management which are further classified across 5 domains. The domains provide objectives, processes and practices for IT governance, risk management and compliance. Organizations can strengthen decision-making, ensure regulatory alignment and improve overall IT value delivery. The governance principle ensures the stakeholder's internal and external need to prioritize resources and decision making. The management principle focuses on planning, building, implementing and monitoring the activities set to achieve the objectives set by governance body ultimately to meet the enterprise goals [17].

3.1.4 NIST Cybersecurity Framework (CSF)

The U.S. National Institute of Standards and Technology developed a cybersecurity framework that is a widely recognized voluntary framework that provides organizations with a structured approach to managing cybersecurity risk. The NIST Cybersecurity Framework, developed by It is built around 6 core functions; Govern, Identify, Protect, Detect, Respond, and Recover, which serve as a high-level taxonomy of cybersecurity activities and outcomes. These functions are further supported by categories, subcategories, and informative references to other standards, making the CSF adaptable to organizations of different sizes and sectors [18].

The framework is risk-based and emphasizes outcomes rather than prescriptive controls, allowing organizations to prioritize investments and tailor cybersecurity practices to their specific risk appetite and resources. Unlike compliance-driven standards, NIST CSF encourages organizations to assess their current cybersecurity posture, define a target state, and develop a roadmap for improvement, making it a flexible tool for continuous cybersecurity maturity development. Research highlights that its structured approach improves communication of risk at executive and operational levels while aligning cybersecurity with business objectives [19].

3.1.5 Centre for Internet Security (CIS) Controls

The Centre for Internet Security (CIS) Controls, originally introduced as the SANS Top 20 Critical Security Controls, provide a prioritized and prescriptive set of cybersecurity best practices designed to help organizations defend against common cyber threats. The framework currently defines 18 high-level controls organized into basic, foundational, and organizational categories, addressing areas such as asset inventory, vulnerability management, secure configuration, access control, incident response, and penetration testing [20]. Unlike broad governance frameworks, the CIS Controls emphasize actionable and technically focused measures that organizations can adopt incrementally to strengthen security posture. One of the core strengths of the CIS Controls is their prioritization and adaptability. The framework adopts an “implementation group” model that categorizes organizations based on size, resources, and risk exposure, allowing smaller entities to start with essential controls and progress toward more advanced measures as their maturity increases.

3.1.6 Kybermittari (Cybermeter)

Kybermittari (Cybermeter) is a cybersecurity framework developed by the National Coordination Centre of Traficom’s Finnish Cybersecurity Centre (NCSC-FI) to help organizations in Finland to assess, identify and implement the cybersecurity measures necessary to protect their data and network infrastructure. The tool is derived from NIST-CSF and the Cybersecurity Capability Maturity Model C2M2 [21]. The kybermittari operationalises a maturity-based approach: it maps organisational capabilities against defined objectives and visualises maturity per domain. The tool is structured so that organisations answer a set of standardised questions that produce a maturity profile, this profile highlights strengths, gaps, and priority areas for improvement.

Organisations complete the kybermittari questionnaire to produce visual dashboards and maturity scores that can be tracked over time. The intended users are managerial and operational stakeholders. The outputs translate technical capabilities into management-friendly indicators and recommended next steps [22]. NCSC-FI has iterated the tool based on user feedback and published support materials and webinars to help organisations interpret results and follow up with concrete measures. Kybermittari is therefore positioned as both an assessment instrument and a management communication tool.

3.2 Frameworks relevancy to SMEs

For SMEs, which often lack formalized security practices, the standard offers a systematic way to define policies, allocate responsibilities, and implement repeatable processes for risk treatment and monitoring [23]. The continuous improvement model embedded in ISO/IEC 27001, via the PDCA cycle enables SMEs to adapt flexibly to evolving threats and regulatory requirements [24]. The complexity of the framework, documentation demands, and certification costs often pose barriers for resource-constrained SMEs [4]. However, studies [24], [4], also highlight that alignment with ISO/IEC 27001 enhances credibility with customers and partners, strengthens compliance with overlapping legal obligations such as GDPR, and helps SMEs build trust in increasingly digital supply chains.

Although the NIS2 Directive is primarily aimed at medium and large organizations in critical sectors, it carries substantial indirect relevance for SMEs through supply chain security requirements and the tightening of incident reporting and risk management obligations [25]. Furthermore, legal and policy analyses highlight that while SMEs may not be directly in scope, the directive indirectly raises baseline expectations for cybersecurity across the EU, creating both compliance burdens and opportunities for SMEs to strengthen resilience, improve market access, and align with best practices [26]. In this way, NIS2 serves not only as a regulatory driver but also as a catalyst for SME cybersecurity maturity and integration into the EU's broader digital economy.

COBIT was originally designed for larger enterprises however, research by da Silva et al. [27] shows that it has substantial relevance for SMEs when used in adapted or scaled forms. A systematic mapping study found that COBIT (versions 4 and 5) is commonly referenced as a best-practice framework in SME IT governance literature, and that successful applications typically simplify or adjust COBIT processes to better match the SME scale, resources, and documentation capacities. COBIT offers value for SMEs as a governance framework that can be selectively adapted. Focusing on the most relevant domains, scaling maturity expectations, and addressing critical risks enables SMEs to use COBIT as a foundation for improving compliance, ensuring accountability, and meeting regulatory requirements.

The NIST CSF offers practical value by enabling a scalable approach to cybersecurity governance that balances resource limitations with regulatory and market pressures. SMEs often struggle with adopting complex frameworks due to limited expertise and cost. However, the CSF's modular design and outcome-based nature allow SMEs to selectively implement

essential practices without requiring extensive resources. Additionally, NIST also provides a quick start guide for small to medium sized businesses with an aim of kick- starting the cybersecurity risk management strategy using the NIST CSF 2.0 [28].

The CIS Controls provide a practical and resource-efficient entry point into structured cybersecurity practices. SMEs often struggle with abstract or resource-intensive compliance frameworks; in contrast, the CIS Controls offer actionable, step-by-step guidance that improves cyber hygiene without requiring significant investment. In the context of SMEs in Finland, where organizations face rising compliance obligations under GDPR and NIS2, the CIS Controls can serve as a practical approach by focusing on core security measures such as patch management, multi-factor authentication, and continuous monitoring, thereby improving both compliance readiness and operational resilience.

Kybermittari is particularly relevant for Finnish SMEs because it offers a scalable and management-oriented entry point into cybersecurity maturity assessment. The tool's emphasis on visual maturity profiles and priority actions helps SMEs that are often constrained by time and expertise to translate abstract regulatory requirements such as GDPR and NIS2 into concrete, staged improvements. NCSC-FI guidance and the SME-oriented materials are intended to lower barriers to assessment by focusing on high-impact, achievable controls first, and by enabling SMEs to show partners and procurers demonstrable progress over time. As such, Kybermittari supports both internal capability building and external credibility in supply chains.

3.3 Role and structure of GRC tools

It has become crucial for all size of enterprises to keep vigilant and manage the ever-evolving cyber threats. The digital landscape of today where business operations are held in complex networks, enterprises need to protect their sensitive data and infrastructures. As discussed above in section 3.1, there are several standards and frameworks that are designed to standardise the process of implementing best security practices through governance, risk management and compliance to achieve cybersecurity. While the standards and frameworks enable and ensure the protection of information systems, it is often challenging for organizations to align the requirements to business objectives. Harmonizing security practices with GRC capabilities benefits operational efficiency and regulatory accountability as organisation scaleup. GRC tools enables a structured framework for management of security efforts while aligning these efforts to business objectives. GRC systems bring together the siloed strategies for managing risks,

adhering compliance and security management into a single platform which helps top-management to make risk-based decisions [29].

The goal of GRC tools is to streamline processes of risks and compliance to ensure that security activities are consistent and enhancing effectiveness. The GRC tools are structured into modules which comprises of interconnected components that support data centralisation and workflow automation. The governance module establishes scope identification, policy frameworks, ownership and leadership reporting leading to accountability for issues and action plans. The risk management module, facilitates assets identification, associated risks identification, risk assessment, action plans to mitigate risks and risk monitoring. The compliance module, ensures defining, monitoring and generating evidence of security activities for adhering to security standards and regulations.

GRC tools also embed incident management along with reporting functions to document security breaches and response. Control mapping and controls testing enable identifying gaps and eliminating redundant controls to increase efficiency of cybersecurity practices [30] . This also helps in creating audit trails and audit reporting. The risk register in the GRC tool can be linked to control assessments that provide metrics for tracking the maturity and effectiveness of implemented controls.

Most of the times, SMEs operate under resource constraints while facing compliance demands from clients. Thus, the role of GRC tools are both significant and challenging in the context of SMEs. GRC tools allows SMEs to formalise the governance process, evaluate risks systematically and reduce manual compliance burdens. However, the complex usability and high-costs of enterprise grade GRC tools cause SMEs reluctant to adopt them [30]. In general, a scalable GRC tool for an SME is essentially a solution that is affordable to start, simple to use, quick to implement showing value, automates manual work and adaptable to changing business, regulatory and technical needs. Table 1 highlights the corre functions of a GRC tool that benefits SMEs for efficient cybersecurity compliance.

Table 1: Core functions of GRC tool

Improve Audit Readiness	Enhance Policy Compliance	Greater Risk Visibility
• Standarise control mapping • Automated evidence collection • Real-time compliance reporting	• Linking policies to controls • Continuous monitoring • Accuracy and traceability	• Real-time risk tracking • Predictive control analytics • Audit performace metrics

3.4 ENISA and EU guidance for SME cybersecurity

The EU is considered the largest single market area and the third largest economy of the world. While large organisations and multi-national companies are attributed to the market size, on the contrary, SMEs in EU act as backbone of the economy. SMEs in EU serve as enabler for digital transformation. Thus, it is crucial to protect data, infrastructure in EU and boost resilience against cyber threats. ENISA was established in 2004 with a goal of achieving a high common level of cybersecurity across Europe. It contributes to cyber policies and guidance to build trustworthiness of ICT products, services and processes. ENISA cooperates with stakeholders (member states, EU bodies) to prepare EU for cyber challenges by sharing knowledge, raising awareness and building capacity.

According to a study conducted by ENISA [3], the majority of SMEs are dependent on information services, processed critical information, used basic security controls, used cloud services for various functions, used remote working setup and are prone to cyber-attacks such as phishing and malware. These characteristics dictate the need of comprehensive cybersecurity guidelines and tools to be implemented by SMEs to secure businesses and citizens of EU. The study also highlighted the challenges faced SMEs in-regard-to applying security practices. The most common challenges were budget constraints, low cybersecurity awareness, inadequate resources, minimal management support and lack of cybersecurity guidelines specific to SMEs.

ENISA provides recommendations across 3 domains: people, processes and technical for SMEs to implement against cyber threats while protecting critical data and infrastructures. The 12-step high level guidelines are [31]:

1. Develop good cybersecurity culture
2. Provide appropriate training
3. Ensure effective third-party management
4. Develop an incident response plan
5. Secure access to systems
6. Secure devices
7. Secure your network
8. Improve physical security
9. Secure backups
10. Engage with clouds
11. Secure online sites
12. Seek and share information

3.5 National Cyber Security Centre Finland

NCSC-FI is a part of the Finnish Transport and Communications Agency (Traficom) which serves as a national CSIRT for Finland. It is also the government Computer Emergency Response Team (CERT) as agreed upon with the Ministry of Finance, Finland. It is responsible for developing and monitoring the operational reliability of security and communications networks and services in Finland. To facilitate this, NCSC-FI maintains situational awareness and network management program throughout the country. It supports resolving cyber incidents, collecting information on such threats, ensuring public communication and secure important functions of the society [32].

NCC-FI officially started its operation in 2023 under NCSC-FI. It is a member of the Network of National Coordination Centres under the European Cybersecurity Competence Centre (ECCC). NCC-FI is dedicated to developing and improving the cybersecurity competence of the operators such as universities, companies and research institutes by facilitating to participate in international R&D works and obtain funding from EU funding programs. According to the report [2], the financial support was streamlined to promote cybersecurity R&D in Finnish

SMEs alongside introducing state-of-the-art security solutions. The financial support is granted especially to SMEs through two different open public call rounds. The report illustrates that a total of 2 million Euros was granted to 50 projects for SMEs. This sort of support encourages SMEs which typically lack budget and resources to invest in a robust and comprehensive security solutions and implement effective practices to secure information and infrastructure.

4 Literature Review

This section aims to review the current state of research on cybersecurity compliance and the use of GRC tools by SMEs to achieving such compliance. Furthermore, it aims to provide a comprehensive understanding of the existing research and knowledge in the area. Despite being a significant economic contributor, SMEs are more vulnerable to sophisticated cyber threats due to limited resources. The issue has become more relevant with regulatory demands such as EU's GDPR and NIS2 directive placing obligations on organisations handling personal data, providing digital services and operating in critical supply chains. The reviewed literatures present a theoretical and empirical foundations for the research focusing on the intersection between cybersecurity standards, the challenges faced by SMEs and the efficacy of the GRC tools. This section synthesises insights from academic, grey literature and industry sources to identify the research gaps in the context of Finland.

4.1 Cybersecurity Compliance in SMEs

Cyberattacks have become more sophisticated technically which dictates the need for robust, comprehensive and effective defensive practices by organisations for information security. Small organisations, however, believe their size makes them less vulnerable to cyberattacks, as shown in a study [33] , 72 % of attacks target small businesses with less than 100 employees. The digital transformation has affected SMEs along with the bigger organisations in regard to cybersecurity vulnerabilities. Cybersecurity discussions are focused more on large organisations however, there is a need of actions to be applied to protect different types of SMEs and better understand the motive of attackers. The research on cybersecurity in SMEs is still limited [34]. SMEs often have limited or lack resources, budgets, expertise and interest from senior management to invest in cybersecurity measures and employee trainings. Hence, cybersecurity compliance is not thought as a strategic priority. Security decisions are often taken by a single person based on intuition who often lack precise knowledge of security standards and frameworks.

Ponsard and Grandclaudon [35], carried out a Strength Weakness Opportunities and Threats (SWOT) analysis on information security governance in small organizations to developing a cybersecurity awareness program for SMEs. Agility and quick response time, alignment with business goals and accessible leadership and willingness to improve were identified as strength. The weaknesses were, digital immaturity, limited resources, overconfidence, low compliance

to security standards and skill management regarding cybersecurity. The opportunities identified were, the GDPR, recognition of cybersecurity as high priority in EU and local initiatives. Lack of cybersecurity experts, unclear recognition of experts and technology advancement was included as threats.

Sendjaja et al. [36], state that cybersecurity is about safeguarding information systems and networks from cyber-attacks aimed to disrupt business operation, modify or destroy sensitive information, or extort users. The advancement of digital technologies has led to increase in the volume of data that are stored and processed online which ultimately increases cyber risks. The interconnected nature of information and network systems have shifted cybersecurity from being a technical function to critical component of business planning and policy development. Cybersecurity now encompasses risks management, protective measures and governance plannings to defend against sophisticated cyber-attacks. Therefore, developing robust and effective cybersecurity strategies that address both present and future security challenges is crucial. The evolution of multiple regulations and standards related to cybersecurity showcase the growing seriousness towards cyber threats. Moreover, a collaborative approach among stakeholders across all sectors and organizational sizes is necessary to develop a comprehensive solution that accommodate diverse compliance requirements and protect information systems and infrastructures.

Organisations are demanded to comply with diverse regulations and frameworks by clients, sector specific bodies and government. Compliance is referred to as process to ensure specific rules and requirements are met. It is often understood that having a regulatory compliance fulfils the cybersecurity requirements for organisations. However, a study by Marotta and Madnick [37] presents that, while regulatory compliance is an integral part of cybersecurity program, it does not complete the cybersecurity measures itself. They define compliance as accountability enabler, assurance function, point of transformation and an ongoing process. Compliance as accountability enabler establishes responsibilities and transparency in implementing processes to ensure a set of rules are adhered. Organisations can demonstrate that they operate in accordance with a defined guidelines and specifications for their sector. This provides sense of assurance and build trust among clients and other stakeholders.

An organisation’s level of practices implementation can change once it moves from non-compliant state to being complaint with a regulation. This shift in state define compliance as a point of transformation for enterprises. Compliance process requires constant monitoring and

periodic checks of applied processes to ensure alignment of business goal with regulatory requirements. Thus, it can be established that compliance which is a part of organisation structure and process is an ongoing process and not a one-time event.

Pawar and Palivela argue in their study [38], that SMEs has been significantly exposed to cyber threats due to digitalisation. However, most of the existing cybersecurity frameworks are unsuitable for their context. The study shows that SMEs operate without formal cybersecurity measures and struggle to adopt to existing standards given the resource constraints of finance and skills to implement traditional frameworks effectively. They also emphasize that leadership's limited understanding of cyber risks hinders prioritising mechanisms to align control with business goals. Pawar and Palivela propose a shift of paradigm from generic one size fits all framework to a tailored business specific approach. The proposed model incorporates principles of the confidentiality, integrity, availability (CIA) triad and defence in depth to determine a phased and maturity-based implementation strategy. By prioritising minimal yet essential controls based on SME's sector domain and critical assets, SMEs can improve their cybersecurity posture while reducing cost and simplifying adoption. Employing shorter, practical assessments rather than demanding full standard compliance to identify highest priority gaps ensures cybersecurity compliance by SMEs while cybersecurity frameworks evolve to accommodate diverse operational environment.

In research conducted by Mitrofan et al. [39], they investigate the underlying factors that make SMEs vulnerable to cybersecurity risks. The digitalisation in business operations have increased vulnerability landscape and cyber-attacks have been targeting small enterprises. Despite, SME owners remain insufficiently aware of cyber threats and are often under prepared to address them effectively. It was revealed by the survey results that SMEs typically exhibited low cybersecurity awareness largely due to limited technical knowledge and insufficient training. The lack of awareness contributes to poor security practices and increases the likelihood of successful cyber-attacks.

Lill et al. [40] conducted a study to address the knowledge gap regarding the specific requirements and practical implementation of cybersecurity practices within the SMEs. It is crucial for SMEs to manage their cybersecurity risks efficiently to protect critical information while remaining competitive. The limited resources and knowledge of SMEs in the area of cybersecurity often make them more vulnerable to increasing number and sophistication of cyber threats leading even to the state of bankruptcy. The result showcased that, security

controls that performed best when implemented fully were given insufficient attention. Lill et al. highlight the importance of investigating the security level of small and medium organisations to identify and analyse the preparedness against cyber breaches. The knowledge of risks assessments and information security measures are vital for determining the security posture, identifying weaknesses and deploying tailored support to the SMEs.

Inadequate defensive mechanisms resulted in SMEs failing to implement basic measures such as regular system updates and structured policies. The resource limitations of small and medium enterprises block them from investigating cyber incidents and breaches that can affect them and other organisations therefore, missing opportunities to learn from them. SMEs also tend to perceive that cyber attackers are only interested in large enterprises which reduces the investment in cybersecurity. While technical controls and mechanisms are essential, cybersecurity education, awareness campaigns and tailored policies are equally crucial for SMEs to adopt a proactive and informed approach to cybersecurity.

4.2 Adoption and Usability of GRC tools

GRC systems are comprehensive software solutions that provide an organization-wide perspective on compliance obligations, risk exposure, and governance goals. These tools generally comprise of modules distributed for risk assessment, asset management, policy management, audit management, internal controls and incident management which provide organisation to have a centralised and easy access to track compliance obligations. GRC tools have become a topic of discussions as they are supposed to bring together technical controls with governance process while meeting business objectives.

This convergence from various perspectives including information-systems architecture, the effectiveness of audits and assurances, regulatory pressures specific to sectors, and the change management of the organization. Security frameworks form the backbone of implementing cybersecurity programs across different organisations in compliance with legal and regulatory requirements. Moreover, a study by M.O. Faruq [30], shows that successful implementation relies not just on the choice of framework but also on the organization's culture, sector requirements, and the expertise on hand.

The ongoing issue of maintaining uniform implementation across varying operational settings continues to be a significant challenge, prompting organisations to pursue organised methods by integrating with GRC platforms. Another challenge in GRC systems is appropriately

distributing resources to make sure essential real-time GRC tasks are not overloaded by unrelated data from ineffective controls. It is crucial to be able to classify risks and ensure risk mitigation strategies are effective in a GRC platform. The integration complexity among data, workflow and reporting oftentimes lead to inefficacy and redundancy at significant costs causing SMEs reluctant for adoption of GRC tools [41]. Both studies by M.O Faruq [30] and Adebayo et al. [41] suggest that GRC tools with capability to combine compliance documentation with operational execution by associating policies with measurable security controls are considered as effective.

Additionally, adoption of GRC tools is also affected by organisational maturity, cross-functional collaboration and support from top management. In today's globalised market, GRC tools are required to have smooth integration between different platforms, customizable interface, easy controls and policy mapping which addresses to difficulties in enforcing policies, evidence collection delays and weak audit trails. GRC tools need to provide capabilities for multi-framework mapping, necessitating an advanced metadata architecture to accurately translate analogous controls between standards without causing duplication or misclassification [30].

Enitan [42], examines the cybersecurity readiness of small and medium-sized enterprises focusing on how resource limitations, policy gaps and low awareness affect their ability to manage cyber risks. A quantitative analysis based on the survey conducted showed that investment in IT infrastructure is the most important factor determining cybersecurity readiness, surpassing general assumption such as policy adoption and employee awareness. Enitan recommends scalable and cost-effective security solutions tailored specifically to SMEs such as modular security tools, formalized polies and access to external cybersecurity support services to address the challenges faced by SMEs. The author argues that these measures can strengthen SME resilience and contribute to the broader security of digital ecosystem.

SMEs face challenges in adopting effective cybersecurity measures while operating without structured practices and the cybersecurity solution developers often lack an accurate understanding of the specific need, constraints and behaviours of SMEs which results in tools that are not aligned with the context of SMEs. Ogunjimi et al. [43], examine this challenge to address the gap and introduce a software named Cybersecurity Coach (CYSEC) that allows cybersecurity experts to define controls and themes that are suitable for SMEs. The software can be used by the SMEs to determine solutions that fit their capabilities and operational

environments. The redundant controls and suggestions in CYSEC were considered complex, impractical and not aligning with SMEs requirements.

The underlying assumption behind the software was that SME's behavioural responses to expert guidance provide valuable indicators of their actual needs and usability constraints. The approach was believed to support more evidence driven understanding of valuable security controls by SMEs. Findings presented by Ogunjimi et al. highlight that SMEs tend to adopt recommendations that are clear, actionable, low-cost, and directly connected to identifiable risks. Moreover, SMEs discarded recommendations that require specialised expertise, significant investment, or major organisational changes, pointing to usability and feasibility issues in current cybersecurity guidance. It emphasizes the importance of tailored solutions to SME environments across diverse business domains.

Vitla [44], investigates how Identity Governance and Administration (IGA) solutions can support an organisation's capacity to meet and maintain cybersecurity compliance. Vitla highlights the key components of IGA such as identity lifecycle management, role-based access control and auditing mechanisms serve as foundational elements to align operational access control with regulatory requirements. Organisations typically face the challenges of scalability, automation and integration with existing enterprise infrastructure. An appropriately designed solution address to these challenges and mitigate cybersecurity risks while simplifying compliance reporting. Vitla presents that incorporating real time monitoring, automated audit trails and assigning privilege-based access reduces unauthorized access and data breaches. These approaches contribute mitigating both outsider and insider threats irrespective of being intentional or accidental. Governance tools such as IGA reduces attack surface by ensuring access of sensitive information and system only by authorized users.

In the context of Finland, it has become common for state sponsored attacks, cybercrimes, Denial of service (DoS) attacks, data leakage and malware attacks amidst being at the forefront in digitalisation internationally. Artificial Intilligences (AI) technologies have enabled new techniques for building threats causing impacts by destruction or disclosure of data for businesses. Some SMEs even had to disrupt operations due to cyber incidents [45]. While some organisations have ensured readiness on cybersecurity others still lack on it, Finnish SMEs still have higher position in cybersecurity in global ranking.

However, golbalisation of businesses have expanded the attack surface and pose challenges for SMEs in achieving comprehensive cybersecurity compliance. Although EU- level regulations

and directive such as GDPR and NIS2 provide a robust preparedness models, SMEs struggle to implement an updated security systems due to limited financing and resources. In the midst of applying traditional security solution such as firewalls and antivirus which are insufficient, bodies like NCC-FI encourage Finnish SMEs to implement a risk based cybersecurity management model like the ISO 27001 standard and NIST framework [2]. Kybermittari (Cybermeter) introduced as local tool by NCSC-FI in Finland shows a shift toward scalable, SME-oriented compliance maturity assessments. However, integration between such diagnostic tools and larger GRC platforms remain limited.

5 Research Methodology

This section presents the research methods used to examine how SMEs in Finland leverage the use of GRC tools for cybersecurity compliance. The study aimed to identify current practices, challenges, and factors affecting the implementation of GRC tools as well as to evaluate the usability and perceived effectiveness of such tools in the context of SMEs. A quantitative survey research design was utilised to collect and analyse data from Finnish SMEs operating in diverse sectors. In addition, an independent analysis of few GRC tools were done based on the usability, compliance coverage, scalability and suitability for SMEs. The combined approach provides both empirical and practical insights into how SMEs can enhance their cybersecurity compliance.

5.1 Research Design

The research adopted a combination of quantitative descriptive design and evaluation of selected GRC tools. The survey provided a systematic description on the current state of implementation, perception and challenges regarding GRC tools in the context of Finnish SMEs while the evaluation method provided an objective view on the functionalities of tools and their suitability for cybersecurity compliance in SMEs. This combined approach allowed this thesis to present the challenges faced by SMEs and how the available tools address to those challenges.

5.2 Population and Sampling

The targeted population for this research were the SMEs operating in Finland (employee numbers ranging from 1 – 249) which processed personal or sensitive data, provided digital services or operated in critical supply chains. The participants ranged from the founder, CEOs, security officers, IT specialists, consultants who were able to provide an indepth understanding on the topic and had atleast a foundation knowledge on cybersecurity and compliance obligations. The targeted number of responses was set to 20 – 30 participants resulting to understand the awareness on cybersecurity and GRC tools use among the SMEs. However, a total of 16 responses were recorded.

5.3 Data Collection

The primary data collection method was the survey, which was facilitated using Webropol, which is known as one of the most versatile survey and reporting tool globally. Moreover, Webropol being originated in Finland, also brought upon a sense of local support and trust especially for conducting a survey involving Finnish SMEs. The survey was distributed using Linkedin, Discord and Personal outreach. The questionnaire available as Appendix 1, was divided among four sections to get insights for the research questions raised in the introduction section of this thesis. The sections were:

1. General information – to understand the context of participating organisations
2. Current cybersecurity & compliance practices – to assess the current awareness and implementation of cybersecurity compliance practices
3. GRC tools adoption – to understand the perception for either adopting any GRC tools or not
4. Perceptions and future intentions – to assess future opportunities for improvement

Additionally, a comparative analysis of few selected GRC tools were conducted to evaluate the relevancy for SMEs. The purpose was to evaluate how the current tools supported the compliance with various cybersecurity frameworks with smooth usability and scalability options in resource constrained environments. Vendor documentation, demo videos and available existing studies were used to collect data. The criteria's used for evaluating the tools were:

1. Economic scalability – to evaluate financial suitability for a growing SME
2. Operational scalability – to evaluate the user experience, interface and automation capabilities
3. Technical scalability – to evaluate technical architecture, integration capabilities
4. Compliance scalability – to evaluate covered frameworks and ease to add and map controls for a new standard
5. Vendor viability – to evaluate trustworthiness of the vendor

5.4 Limitations

Firstly, the sample size used by this study does not provide a full representation of the diverse and broader operational realities of SMEs in Finalnd. The limited outreach and participation of the SME representatives restricts the generalisation of the findings. These constraints may underrepresent the perspective of SMEs that have either advanced or less developed cybersecurity practices. Secondly, the evaluation conducted on the GRC tools was based on the secondary documentations such as vendor materials websites and product descriptions. This may not represent all the functionalities of the final or updated versions of the tools accurately. Certain features and limitations may not be fully captured without a direct hands-on testing and demonstration of the product. However, the combined research approach provides a balanced foundation for analysis. This study also enables a comprehensive understanding of cybersecurity governance, risk management and compliance practices within Finnish SMEs by including multiple data sources and perspectives.

6 Results and Findings

This section presents the results and findings from the survey and the analysis of 4 selected GRC tools. The goal was to evaluate the cybersecurity compliance practices and the use of GRC tools in Finnish SMEs. The purpose of the survey was to understand and quantify the awareness, challenges and perception of the SMEs in Finland regarding cybersecurity compliance and the use of GRC tools. In addition, a comparative analysis was conducted to identify market segmentation between open-source, customizable platforms and commercial, automation-focused solutions, each presenting a distinct set of trade-off for potential SME adopters.

6.1 Survey results

A survey was conducted to understand and quantify the awareness, challenges and perception of the SMEs in Finland regarding cybersecurity compliance and the use of GRC tools. Since the targeted participant groups were the representatives from a specific sectors (organisations that process personal data, provide digital services or operate in critical supply chains affected by the NIS2 directive), only a limited number of responses were recorded. However, the survey provides a basic level of insights on the state of cybersecurity compliance and adoption of GRC tools for it.

A total of 15 questions were presented in the survey questionnaire and divided among 4 sections to get answers to the research questions raised in the thesis. The purpose of section 1 was to understand the context of participating respondents, organisations and their relvance to the research topic of this thesis. Section 2 was designed to explore the current state of cybersecurity frameworks awareness, challenges and compliance practices among the participating SMEs. The potential reasons for either using or not using a dedicated GRC tool for cybersecurity compliance by SMEs in Finland were identified in section 3 of the survey questionnaire. Finally, the questions in section 4 were dedicated to understanding the attitude and expectations of Finnish SMEs towards improving cybersecurity compliance.

6.1.1 Section 1: General information

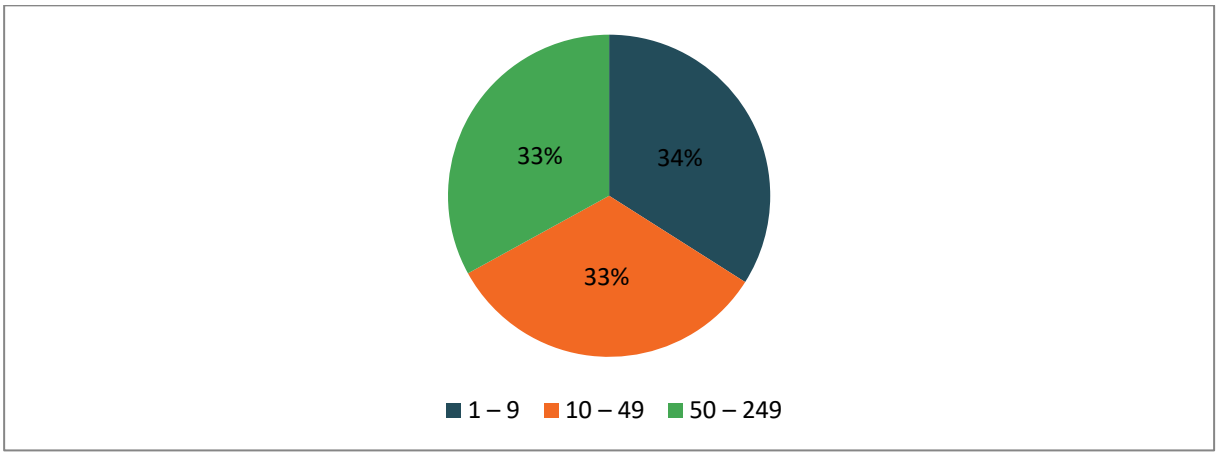

Figure 1:Size of organizations.

The pie chart in Figure 1 illustrates that an equal number of participants responded from each category of SMEs with micro-enterprises (1-9 employees), small-sized enterprises (10-49 employees) and medium-sized enterprises (50-249 employees). Each representing approximately one-third of the total sample, allows for comparative analysis across different sizes of organisation within the SMEs in Finland.

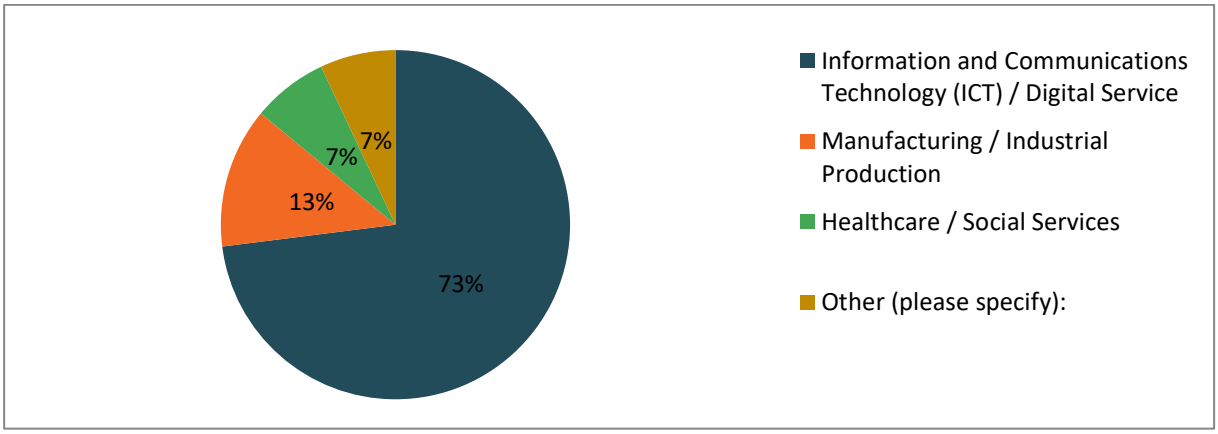

Figure 2:Industry sectors of respondent organizations.

Figure 2 illustrates that a significant number of respondents represented the organisations operating in ICT and digital services with 73% of the total sample. 13% of participants operated in manufacturing and industrial production sector while industry sectors from health/social services and other had equal representation of 7% each. The other sector was organisation providing cybersecurity services. Moreover, none of the participants from finance/insurance and energy/critical infrastructure sectors participated in the survey. This distribution reflects

the profile of Finnish SMEs that are most engaged and affected by modern cybersecurity compliance standards and regulations.

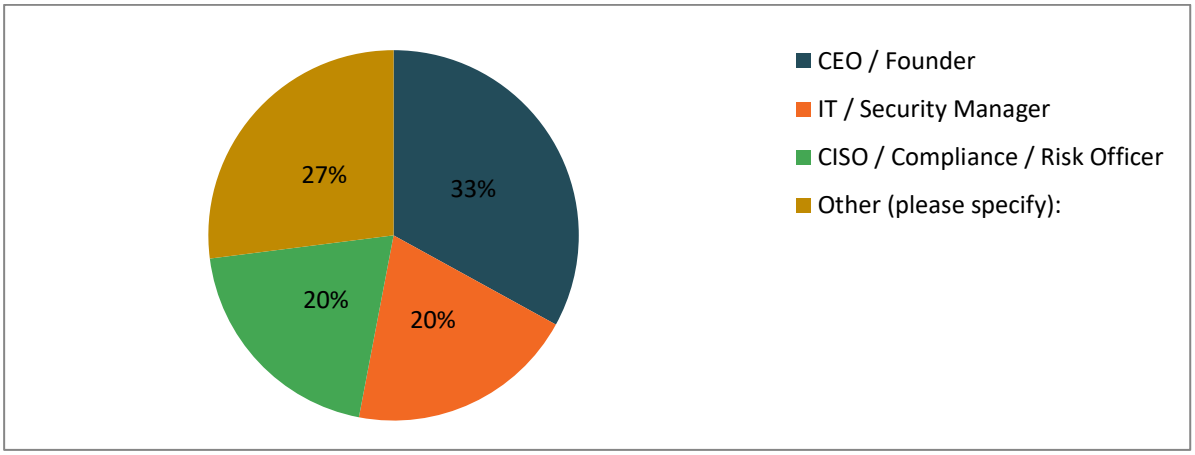

Figure 3:Roles of respondents.

Most of the respondents taking the survey were the CEOs or Founders with 33% of the sample. Among the respondents, 27% of participants mentioning others as roles were IT and Security heads, CPO/CISOs and IT specialists. As shown in figure 3, dedicated security professionals such as CISO/Risk officers, IT/Security Managers also responded to the survey. The data illustrates the perspective of individuals from both spectrum the strategic oversight and technical responsibility.

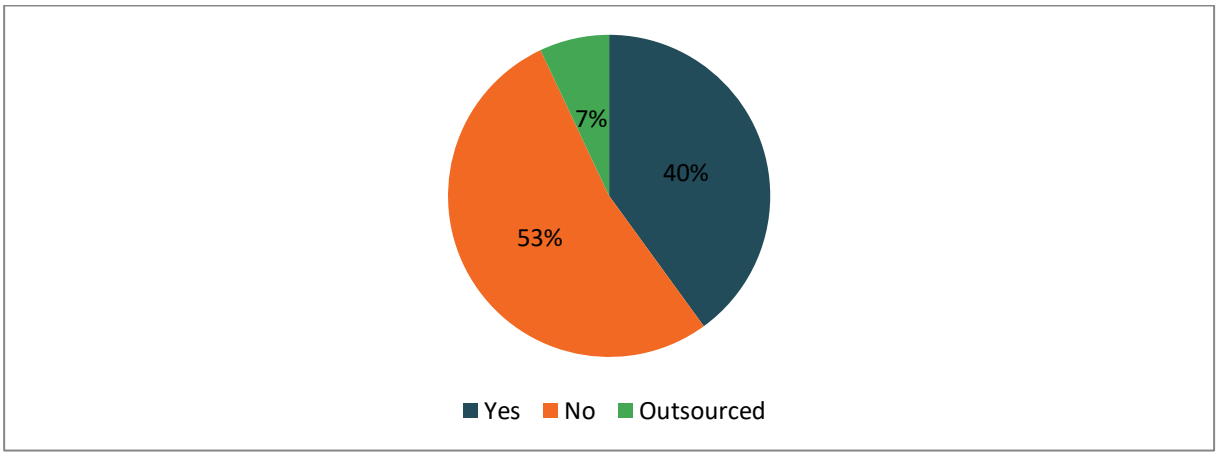

Figure 4: Dedicated cybersecurity function or department.

The result in figure 4 shows that majority of the SMEs, 53%, did not have a dedicated inhouse function or department to carry out the cybersecurity related activities. While 40% have a dedicated function, 7% outsourced their cybersecurity compliance to vendors.

6.1.2 Section 2: Current state of cybersecurity & compliance practices

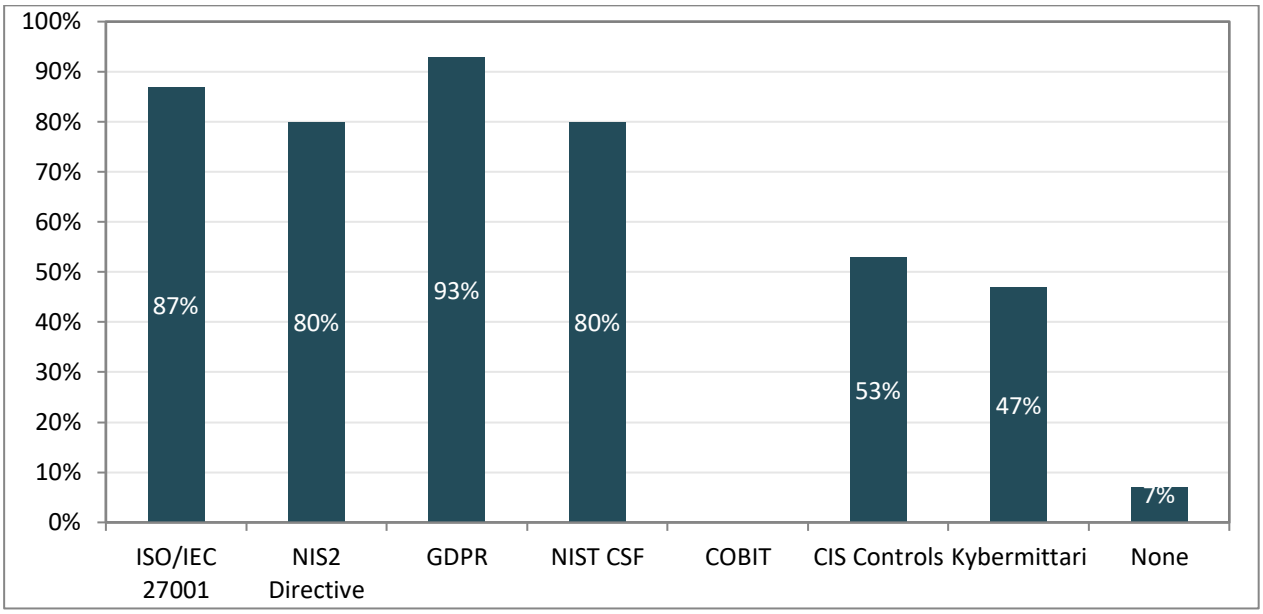

Figure 5:Cybersecurity frameworks awareness.

When asked about the familiarity among participants about different cybersecurity frameworks and standards, the result indicated that majority of individuals were aware about multiple frameworks. The data in figure 5 shows 93% knew GDPR and 80% were familiar with the NIS2 directive which are most relevant to Finnish SMEs. Significant numbers were familiar with the ISO 27001and NIST framework which are the most common frameworks globally. Despite being a domestic tool, only 47% of participants were aware about Kybermittari which indicates a communication gap between Finnish SMEs and NCSC-FI.

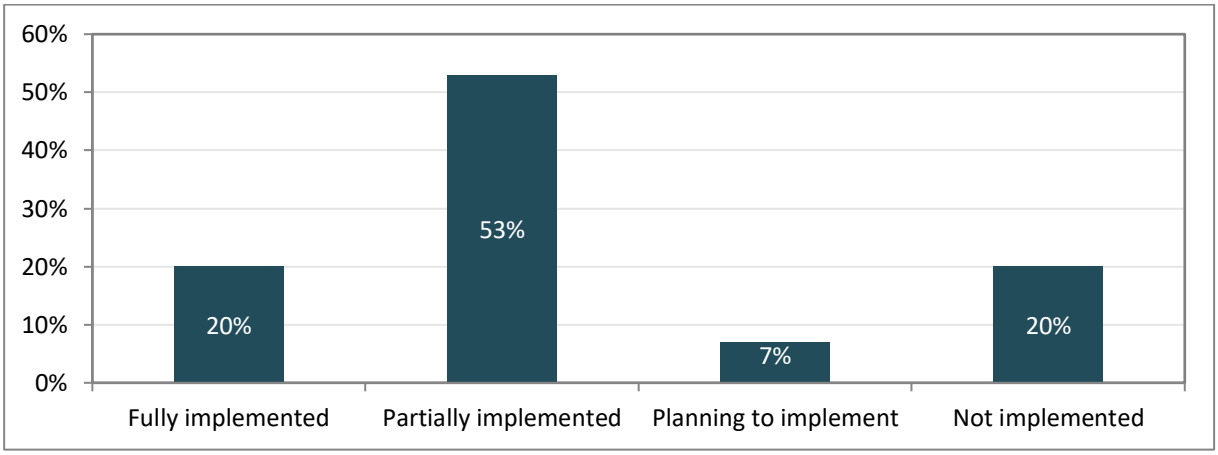

Figure 6:Framework implementation.

The data in figure 6 illustrate that 20% of the participating SMEs fully implemented any of the cybersecurity framework in their organisation while the other 20% did not implement any of those. While few had framework implementation plans in future, some did it partially.

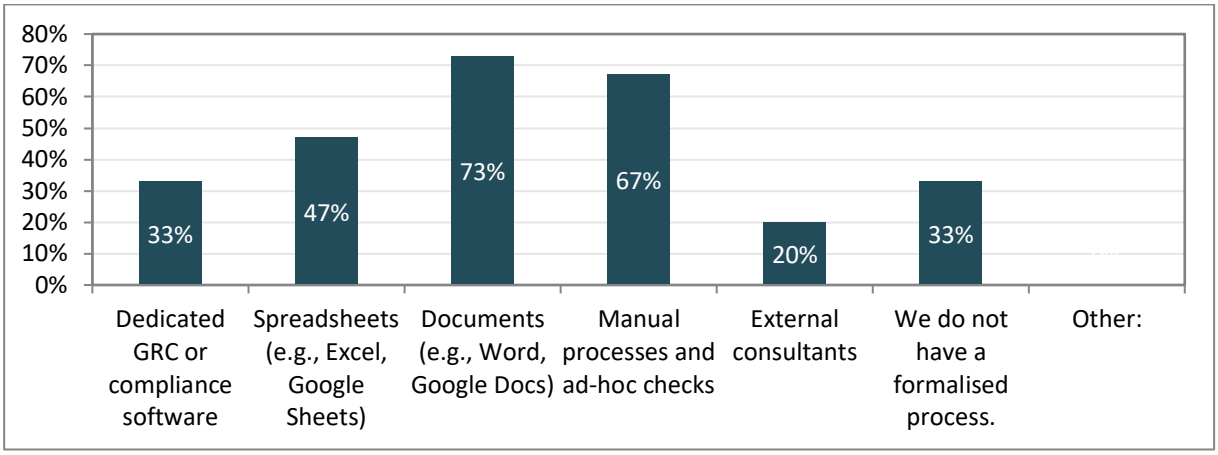

Figure 7:Managing compliance activities.

Survey results shown in figure 7 indicate that cybersecurity compliance in Finnish SMEs is primarily managed through manual methods. Spreadsheets are the most common tool, underscoring a significant reliance on informal and fragmented processes rather than dedicated GRC software or structured external support.

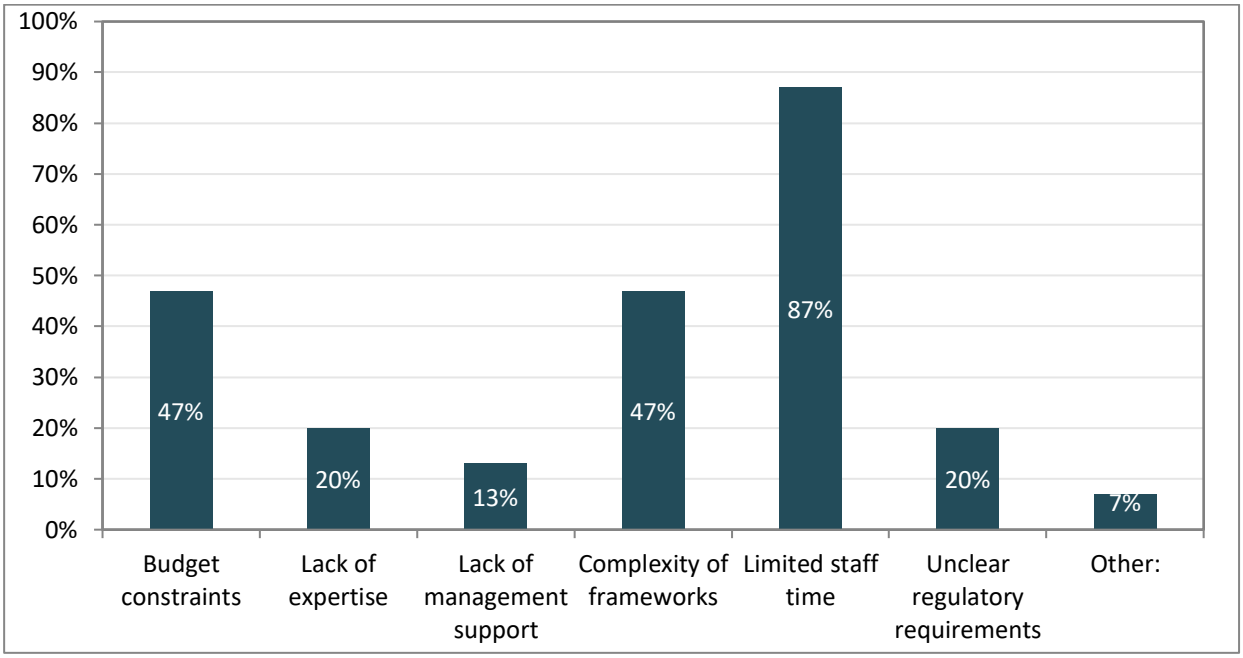

Figure 8:Challenges affecting cybersecurity compliance.

As illustrated in figure 8, the complexity of frameworks, limited staff time and budget constraints are the most popular challenges affecting cybersecurity compliance. While 20%

indicated lack of expertise, about similar number mentioned lack of management support hindering compliance within the Finnish SMEs.

6.1.3 Section 3: Adoption of GRC tools

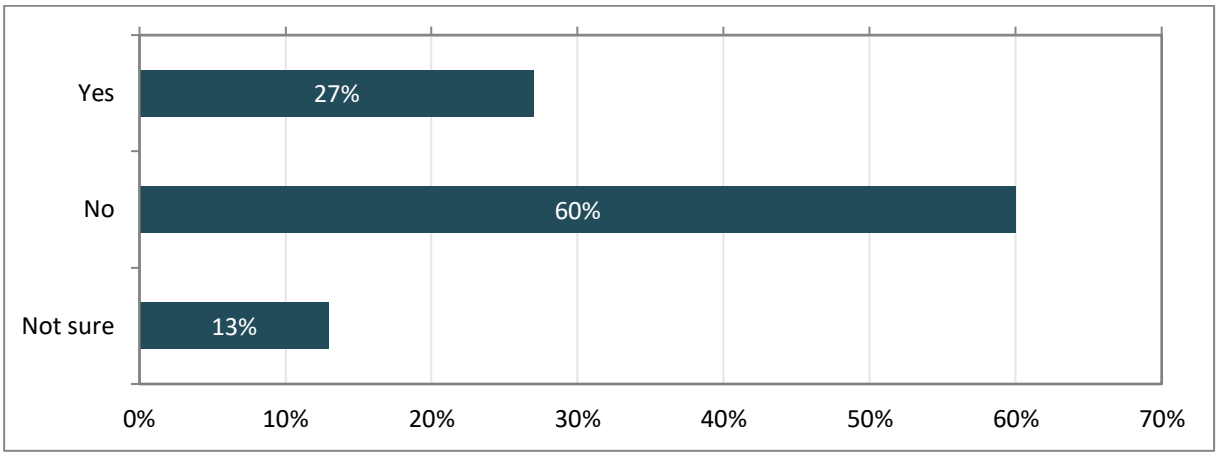

Figure 9:GRC tool adoption.

Figure 9 shows that a significant majority of participating organizations (60%) reported not using a dedicated GRC tool. Only 27% have adopted such a platform, while 13% are unsure. This indicates that the market for dedicated GRC solutions in the Finnish SME sector is still in its early stages, with substantial potential for growth.

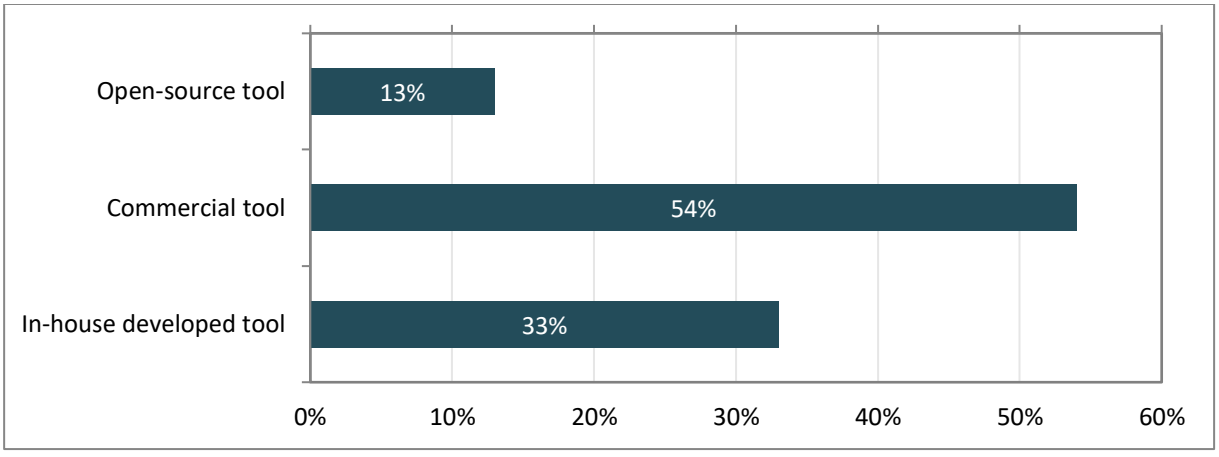

Figure 10: GRC tool used in participant's organization.

Among the small number of organisations adopting any GRC tools, 54% used a commercial tool for compliance management activities. The data in figure 10 show that a good proportion relying on in-house developed tools while some used open-source tools. The result indicates that the Finnish SMEs adopting to GRC tools seek support and structure provided by commercial vendors rather than developing or using a free community supported option.

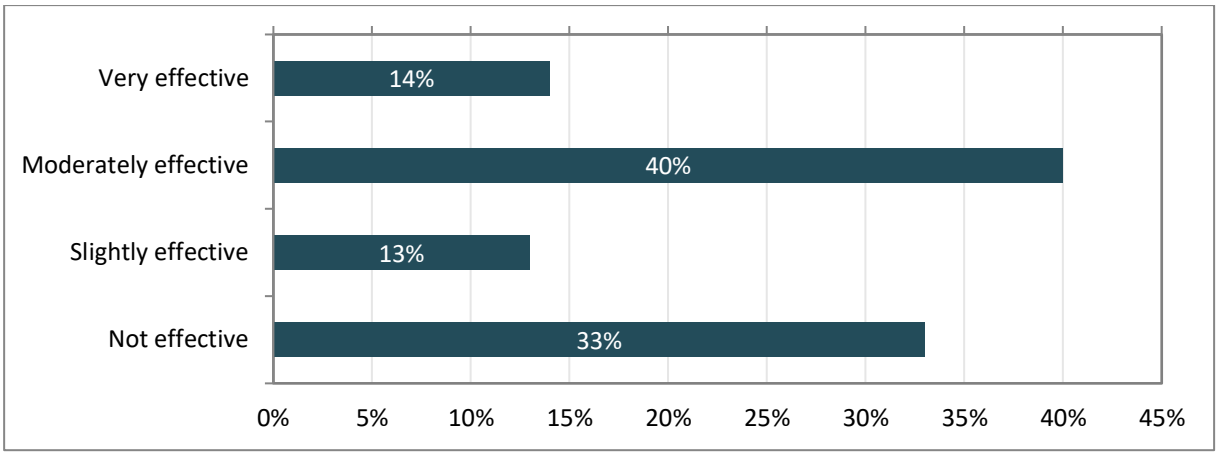

Figure 11: Effectiveness of GRC tools.

While majority of respondents found adoption of GRC tool to be at least "Moderately effective", one-third of the respondents still thought implementing any GRC tool did not affect the compliance management at all as illustrated by figure 11. This shows the need for tools specifically tailored for SME context.

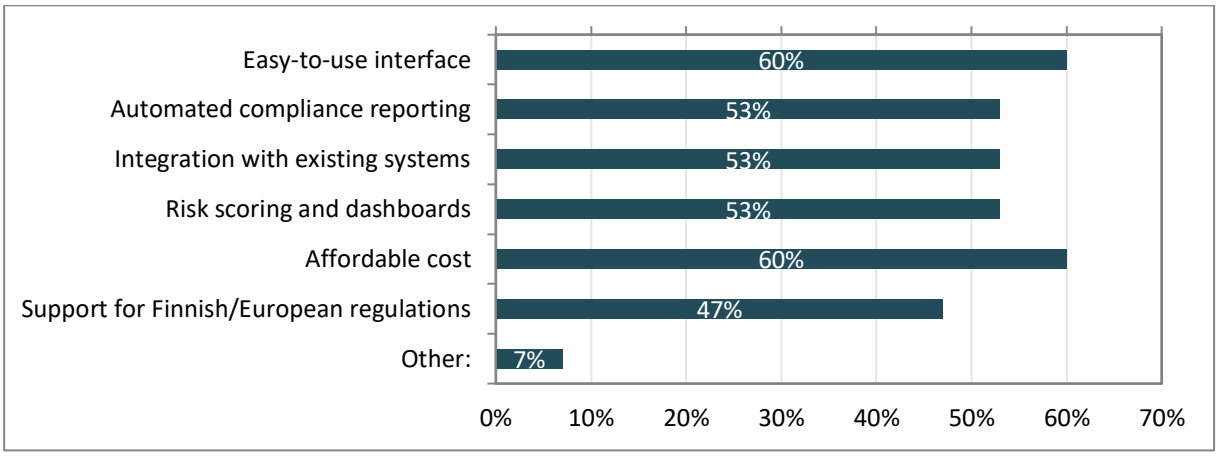

Figure 12: Expected features in GRC tools.

Figure 12 illustrates that the most critical features for SMEs in Finland are the easy-to-use interface and affordable costs as responded for by 60% of respondents. Risk scoring dashboards, automated compliance reporting and integration are also the desired key features which are crucial for smooth scaling up. Among the responding participants, 47% indicated tools with features for supporting Finnish and European regulation showcasing the need of regional relevance of the tool among others.

6.1.4 Section 4: Perception and future intention

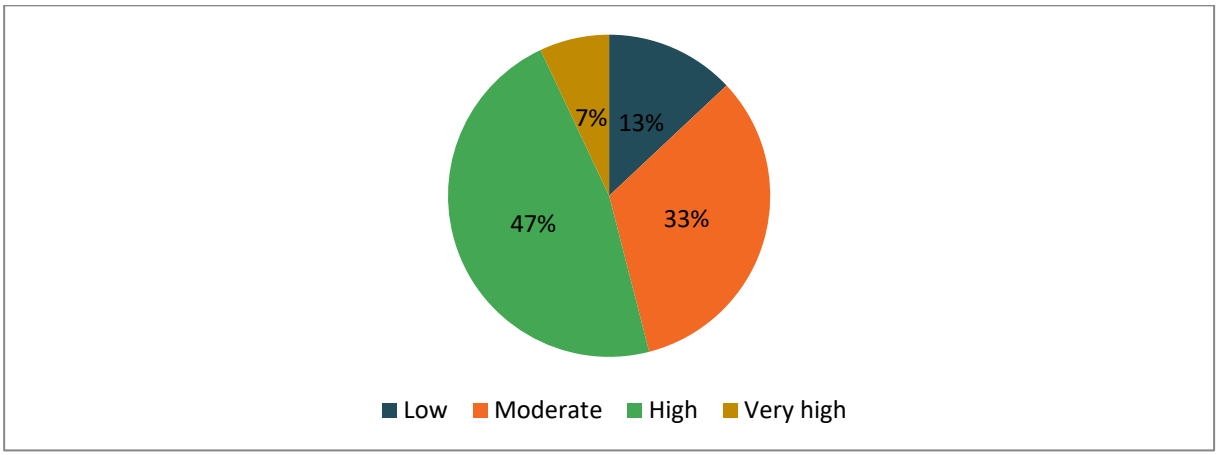

Figure 13: Perceived cybersecurity maturity level.

According to the result shown in figure 13, 47% of the respondents believed that they have high level of cybersecurity maturity in their organisation while a small fraction perceived to have very high maturity level. The data shown in figure 13 illustrates that 13% thought they had a low cybersecurity maturity level indicating gap in the cybersecurity posture within the SMEs.

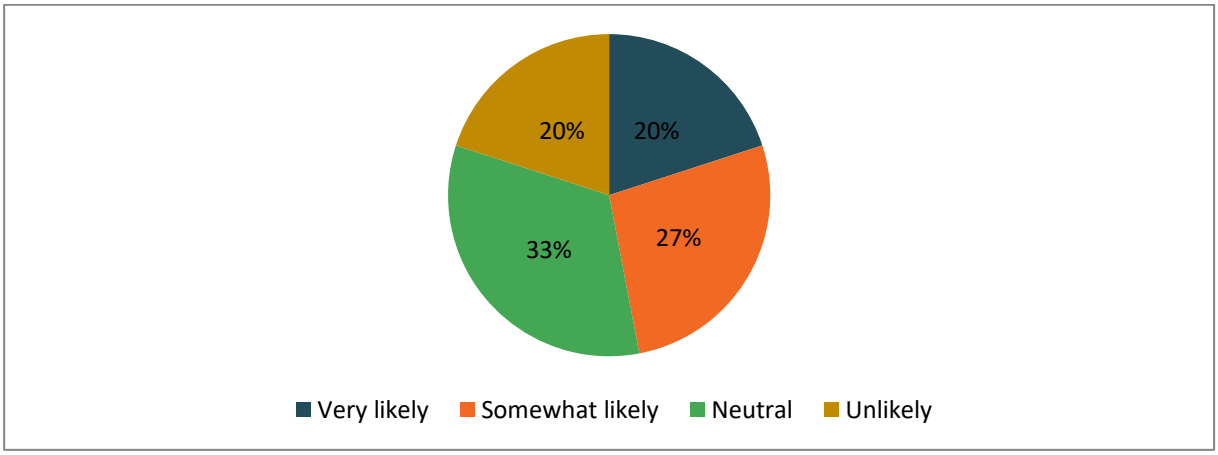

Figure 14: Likelihood of investing in framework or tool.

A combined 47% of participants showcased that they are likely to invest in cybersecurity frameworks or tools in future while a significant portion were uncertain (33%) or not (20%) making any investments. This result showcased by figure 14 suggests that Finnish SMEs are still hesitant implementing cybersecurity management solutions given the significant barriers.

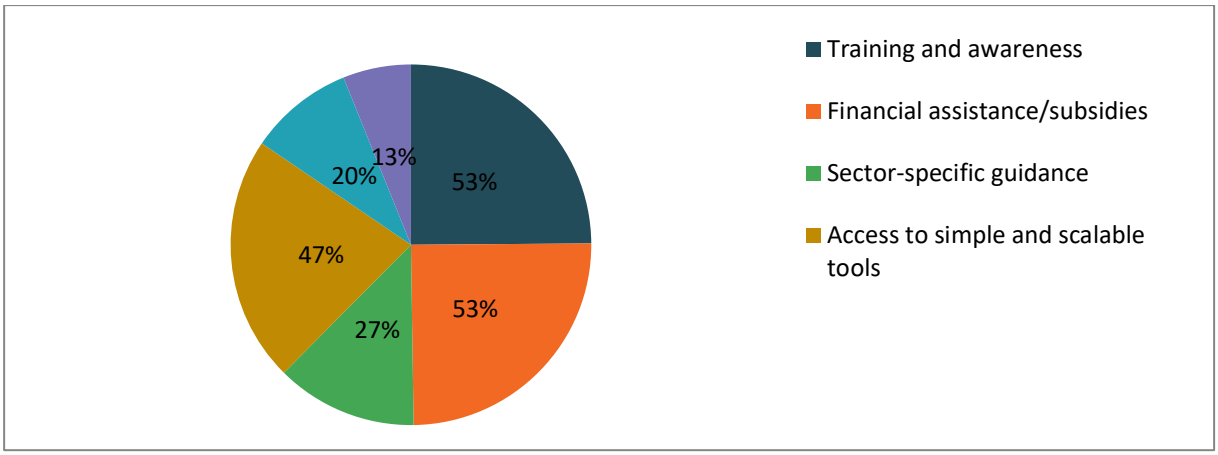

Figure 15: Perceived support for tools implementation.

The result from the survey in figure 15 illustrates that financial assistance along with effective training and guidance at 53% are most valued support needed to improve cybersecurity compliance. Followed by demand of sector-specific guidance and expert consultancy, SMEs perceive critical for implementing cybersecurity framework or tools. This strongly indicates that SMEs in Finland struggle with costs and complexity adhered by cybersecurity solutions for enhancing their cybersecurity posture.

In summary, Finnish SMEs participating in the survey are highly aware of globally recognised cybersecurity frameworks but less known about free domestic tool for assessing and organising cyber practices. This indicates the need of mechanisms by dedicated organisations like NCSC-FI to educate SMEs extensively about the provided tools and guidelines. The survey result illustrated that cybersecurity compliance is primarily managed through manual efforts which indicates market gap for automation. The primary challenges to tool adoption are high costs, complexity of frameworks, lack of sector specific features of the tools. It was noticed that the SMEs in Finland wish to have a solution that has user friendly interface, affordable costs and support for regional regulations. The adoption of a GRC tool is based on financial support from government authorities and the scalability option provided by the tools.

6.2 Comparative analysis of GRC tools

A comparative analysis of selected 4 available GRC tools was performed to evaluate how they meet the needs of SMEs in cybersecurity compliance and whether they are scalable. As mentioned in section 5.3, the selected tools were evaluated based on the five criteria: economic scalability, operational scalability, technical scalability, compliance scalability and vendor viability. The tools were chosen to represent the spectrum of solutions available to SMEs. The

selected tool represents open-source, commercial open-source, global automated, and regionally specific solutions. The tools capture the core trade-offs between cost, customisation, automation, and local expertise.

Table 2 presents the findings from the comparative analysis of the selected four GRC tools, providing a clear and structures overview of how each solution aligns with the need of Finnish SMEs. It highlights the relative strengths and weaknesses of each tool against the determined evaluation criteria by systematically assessing them. The evaluation criteria, economic scalability, operational scalability, technical scalability, compliance scalability and vendor viability were chosen to reflect the multifaceted needs of Finnish SMEs that are cost-effective, easy-to-use, technically adaptable and compliance supportive solutions backed by relaible vendors. The overview serves as an analytical foundation for the recommendations that follow, supportive evidence-based decision making to GRC tool adoption.

6.2.1 Open GRC

Open GRC is a free open-source web-based tool designed to manage security programs for small businesses for cybersecurity compliance. It covers a broad range of frameworks such as the ISO 27001, NIST and COBIT. However, the implementation, mapping and maintenance require robust configurations. Open GRC requires user with some technical skills and prior GRC experience. While integration to existing systems is possible via APIs, scalability is constrained by significant customisation requirement. Being a community driven platform, the tool lacks formal vendor support and is dependent on community forums and documentations. Although the tool itself is free, the adoption can be costly for server hosting, maintenance and expertise required for configuration and management [46].

6.2.2 Eramba

Eramba is also a solution designed to address GRC for SMEs. It offers both, free open source community edition and the paid enterprise edition with extended functionalities. Similar to Open GRC, Eramba also supports multiple frameworks making it a comprehensive GRC tool with built-in modules for risk management, compliance, audit and incident tracking. The user interface is easy to use and structured with dashboards and risk visualisation however requires some technical knowledge for initial setup. It offers better integration through APIs and also for automated data pulls from other systems. Having a paid enterprise edition, Eramba provides an active support and services [47].

6.2.3 Sprinto

Sprinto is a cloud-native GRC platform primarily focusing on hig demand compliance standards such as ISO 27001, SOC 2, GDPR, PCI DSS and HIPAA with an option to expand to other frameworks. The pre-built programs, control library, policies and automation reduces setup times by simplfying compliance especially for SMEs. Sprinto offers integration with over 200 cloud applications and services making it highly scalable in addition to a subscription based pricing along with dedicated customer service. In addition, it provides a high level of security assurance implementing regular audits, compliance validation and continuous monitoring [48].

6.2.4 Cyberday

Cyberday is a GRC tool developed in Finland tailored to address the needs of SMEs covering a vast range of compliance frameworks such as ISO 27001, SOC 2, NIS2, GDPR and other EU regulations. The tool offers a modern user-friendly interface with visualisation dashboards, guided tasks automation, risk managemnt workflows and more. Cyberday GRC tool integrates with MS teams and slack for user integration, reminders, tracking and ease of access. It aslo offers a subscription based pricing model based on the size and need of the organisation. It provides a robust customer service and has solid reputation locally and in the nordics. Cyberday ensures secure data handling complying with security standards and EU- regulations [49].

Table 2: Comparative analysis of selected GRC tools.

Evaluation Criteria	**Open GRC**	**Eramba**	**Sprinto**	**Cyberday**	**Rational and Implications for Finnish SMEs**
Economic Scalability	Free, but high setup and maintenance cost	Both (free and paid editions), medium initial setup cost	Subscription based and low setup cost	Subscription based and low setup cost	Open GRC and Eramba are suitable for SMEs with inhouse technical expertise while Sprinto and Cyberday have lower running costs

Operational Scalability	Basic user interface, requires self-building of control libraries	Structured interface, built in modules but requires technical expertise	Modern and easy to use interfaces with pre-built templates and multiple use cases	Modern and easy to use interfaces with pre-built templates and multiple use cases (EU-focused)	Open GRC and Eramba require dedicated and technical experts. Sprinto and Cyberday are easy to use for users from any domain
Technical Scalability	On-premise, Limited integration possibilities	On-premise and SaaS, better integration	Cloud-native SaaS, extensive integration possibilities	Cloud-native SaaS, extensive integration possibilities	SaaS tools are more favourable for scaling effortlessly
Compliance Scalability	Supports multiple frameworks but requires manual effort for configuration	Supports multiple frameworks but requires manual effort for configuration for free version	Supports multiple frameworks, automated control mappings and compliance processess	Supports multiple frameworks, automated control mappings and compliance processess strongly aligned with EU regulations	Cyberday can be more favourable in the context of SMEs in Finland especially seeking compliance with NIS2 directive
Vendor Viability	No dedicated customer support, community based learning and documentations	Community support for free edition and limited customer support for eterprise edition	Dedicated customer support	Dedicated customer support	Commercial vendors have low risks with formal and dedicated support process

7 Discussion

This section synthesizes and interprets the key findings from the empirical study comprising the literature review, the survey of the Finnish SMEs and the comparative analysis of GRC tools to address the research questions. The aim is to provide a coherent explanation of the factors influencing the adoption of scalable GRC tools using the theoretical insights, the survey data and analysis of solutions. The section further interprets the practical implications of the comparative analysis of GRC tools in relation to the need and constraints identified through the literature review and survey results. This discussion provides a deeper understanding of how scalable GRC solutions cab enhance cybersecurity compliance among Finnish SMEs.

RQ1: What are the primary challenges that SMEs in Finland face in achieving cybersecurity compliance?

Among many challenges the SMEs face due to limited resources, expertise and complex regulations, cybersecurity compliance challenges are critical. SMEs mostly have minimal budget and staff for security which reflects to lack of dedicated or core function for cybersecurity and compliance. This aligns with a study by Lill et al. [40], where they mention that “limited knowledge and resources in this area” make SMEs vulnerable even leading them to a state of bankruptcy due to a successful cyber-attack. These limitations often result in use of manual and ad hoc processes. Such practices depend on managerial experiences rather than area expertise which leads to higher compliance costs, inefficiency and difficulties to keep updated on changing regulations [9].

Additionally, the complexity of frameworks and robust regulatory requirements also pose a challenge of SMEs to comply. The landscapes are diverse and continually changing regulations make it difficult for SMEs to adapt practices to their workflows [9]. Finnish SMEs struggle with the complexity of frameworks and unclear regulatory requirements for cybersecurity compliance. In summary, the challenges are not siloed but are interconnected. Limited resources compel the use of manual processes which do not favour navigating complex regulation requirements and ultimately increases costs when fixing damages caused cyber incidents.

RQ2: What frameworks and tools currently support SME GRC efforts?

The landscape of available frameworks and tools to Finish SMEs is characterised by a critical disconnect between availability and applicability. The survey indicated that Finnish SMEs who

are generally aware of international and regional cybersecurity frameworks however, the implementation largely remains partial showing adoption gap. This signifies the challenge of complex framework and the need for simplified, small enterprise-oriented tools for compliance [19]. A large portion of SMEs in Finland participating in the survey did not use any GRC tools for cybersecurity compliance. Robust GRC frameworks are intended to provide a structured approach the needs of organisations including SMEs. They provide a clear roadmap for developing policies, assessing risks and audit processes [50]. The NIST CSF even provides a lighter version specific to small businesses.

The comparative analysis of tools presented the availability of free and commercial GRC solutions focusing on SMEs. Tools like OpenGRC and Eramba offer a free community versions with basic interface and decent coverage of security standards however, the setup and customisation required by these tools demanded technical expertise. Sprinto and Cyberday provided subscription-based pricing with better scalability. The costs associated can still be high for SMEs to invest in cybersecurity. The analysis underscores a market gap in terms of tools balancing both economic and operational scalability. This aligns with the notion made in study [25], that noted the lack tailored cybersecurity frameworks for small enterprises.

RQ3: How effective and usable are these tools in real-world SME environments?

A GRC tool can be considered effective when it reduces risk without overburdening the business. A properly implemented tool can automate routine tasks while improving compliance. An automated compliance tool with pre-configured templates improves regulatory adherence and supports maintain high level of governance [25]. Finnish SMEs mostly considered using a GRC tool or framework is ineffective, and few found the tools slightly to moderately effective as shown in figure 11. The finding suggests the frameworks and tools are only effective if they match the capacity of SMEs.

The open-source and freemium models offered by OpenGRC and Eramba incorporate high economic scalability but presented low operational scalability with setup, customisation and maintenance demands requiring technical expertise and more staff hours. However, these tools can be beneficial for SMEs with inhouse experts. Modern GRC tools such as Sprinto and Cyberday often offer step by step onboarding and integration guides to simplify compliance management. The complexity of integrating data, workflows, and reporting often results in inefficiencies and duplications at substantial costs, which makes SMEs hesitant to adopt GRC tools. Research [41] indicates that GRC tools that can merge compliance documentation with

operational execution by linking policies to measurable security controls are viewed as effective.

RQ4: What factors influence the adoption of GRC tools among SMEs?

There are several factors influencing the adoption of GRC tools among SMEs. The presented survey results indicate affordable cost as one of most important factors for adoption. License fees, implementation expenses, need for expert training or external consultant and other hidden costs deemed as high compliance cost can act as barrier for small and medium enterprises in adopting a GRC tool [40]. Easy-to-use interface is another factor that influences SMEs to implement a GRC tool. A solution that requires less time on training and easy to navigate can encourage SMEs to adopt a GRC tool for compliance. Guided integration feature and reliable customer support provides SMEs with a sense of confidence and trust from vendors. Moreover, risk scoring dashboards, integration possibility, automated compliance reporting were other features that affected the decisions for SMEs.

A tool that supported Finnish and other EU regulations was also indicated as desired feature by Finnish SMEs. When asked about the likelihood of investing in a tool for compliance, a combined 47% of the respondents showed interest and the other 33% stayed neutral. This indicates the neutral group is not aware enough about the benefits implementing a GRC tool can provide. In summary, adoption of GRC tools in SMEs is driven by cost-benefit calculations, user friendliness with integrated risk and compliance workflows whereas, uncertain value and steep learning curves contribute to resistance [25].

7.1 Practical implications

The findings present several practical implications for Finnish SMEs, vendors and policymakers. The survey results underscore issues on the approach of SMEs towards cybersecurity governance, risk management and compliance. These implications highlight the trends in practical operational contexts. The survey shows that SMEs remain constrained by limited financial resources, lack of expertise and strong reliance on manual ad hoc processes for compliance. These limitations hurdles SMEs when navigating through complex regulatory requirements. SMEs become more exposed and risk prone due to dependence on managerial experience rather than domain expertise leading to inconsistent governance practices. The direct practical implication is that manual compliance practice is not sustainable for SMEs. SMEs relying on unstructured and undocumented processes are subjected to face operational,

financial and legal burden as the regulatory requirements evolve. The findings imply an urgent need for SMEs to adopt to structured and partially automated compliance practices to improve resilience.

The reviewed literatures and the survey results in this thesis reveal a gap between framework awareness and implementation. Actual implementation is fragmented despite SMEs recognising international and regional standards such as ISO27001 and NIS2. This demonstrates that existing frameworks are perceived as complex, resource intensive and poorly aligned with the realities of SMEs. The framework applicability is more significant than framework availability. SMEs need simplified, sector specific interpretation of cybersecurity standards or tools that can translate complex framework requirements to manageable tasks. Initiations from national bodies such as Kybermittari (Cybermeter) remain underutilized due to low awareness which suggests need for stronger outreach and communication from public authorities.

The comparative analysis illustrates a gap between the economically scalable and operationally scalable GRC tools. On one hand, the open-source and freemium tools offer a low-cost entry points requiring technical expertise which many SMEs lack and on the other hand, commercial SaaS tools provide enhance usability and support but at a higher cost. The practical implication is that there is no single category of GRC tools that meets all SME needs. SMEs with in-house technical capabilities can benefit from free tools whereas, the ones without vast technical capabilities require intuitive, guided tools struggle with costs. This implies that the effectiveness of the tools does not depend only on features but on the capacity and maturity of SMEs.

Several adoption factors such as cost-effectiveness, usability, scalability, automation and compliance with Finnish and EU regulations were identified as the factors affecting decision-making of SMEs. A notable number of respondents showed either interest or neutrality to investing in GRC tools which suggest that they are not resistant but more uncertain about tangible value provided by GRC tools. The practical implication is that demonstration of reduced audit burden, automated evidence collection and reporting, moreover, return value on investments are necessary to convert neutrality to adoption. SMEs, having limitations by resource constraints evaluate tools primarily through cost-benefit prospect. This must be acknowledged by vendors and policymakers.

The findings from the survey conducted for this thesis show that Finnish SMEs are comparatively less aware about the domestic tool like Kybermittari and other guidance despite being useful and cost benefit. This indicates that public sectors and authorities must enhance visibility and usability of national and regional cybersecurity resources. National bodies like Traficom and NCSC-FI can play a more active role in supporting SMEs through awareness campaign programs.

Overall, the results of this research suggest that addressing cybersecurity compliance in Finnish SMEs require more than offering tools or frameworks. It suggests coordination amongst SMEs, vendors and policymakers to reduce complexity, improve usability and strengthen awareness. GRC tools must be affordable, automated and tailored to needs of SMEs to drive adoption and improve cybersecurity posture. Cybersecurity compliance can be transformed from burdensome activity into resilience building practice for SMEs by addressing the interconnected challenges of resources and tool design.

8 Recommendations

This section suggests actionable recommendations for SMEs, GRC vendors and policymakers to enhance cybersecurity compliance. Based on the insights from the survey findings, comparative analysis of tools and previous academic studies, this section aims to translate this study's conclusion into clear strategic directions that address identified challenges such as resource limitations, framework complexity and low tool adoption. The recommendations are designed to support SMEs in selecting and implementing effective GRC solution, guide vendors in developing SME targeted features and inform policymakers on enabling support and access to cybersecurity education and tools. This section provides practical, evidence-based suggestions to strengthen cybersecurity practices promoting the adoption of scalable GRC tools.

8.1 For SMEs

SMEs should begin to understand their organisational needs clearly. This includes identifying core business requirements, critical assets, stakeholder expectations and regulatory obligations before adopting any tool or framework reactively. As highlighted in prior studies [3], [35], focusing on core business and assessing what needs protection are the key for establishing effective SME cybersecurity practices. SMEs should adopt a risk-based and phased approach to compliance. Beginning with a set of prioritised controls and scaling up gradually towards comprehensive frameworks, organisations can manage workloads in realistic and sustainable way.

SMEs should prioritise tools with core functions such as risk assessment and management, pre-built policy and process templates, automated framework mappings and reporting. These functions help to create structure and simplify complexities of compliance tasks. The GRC tools that integrates seamlessly with existing systems and enable future expansion through APIs and automation capabilities are important considerations for SMEs. These features minimise manual work, reduce tasks duplication and decrease long-term operational costs. Additionally, these capabilities can transform compliance from a fragmented, reactive approach into streamlined proactive function that enhances the overall security posture of the organisation.

The SMEs which lack inhouse-technical expertise in particular, should prioritise tools with intuitive interfaces, guided workflows and minimal configuration needs. This reduces training times for staffs which encourages consistent engagement with cybersecurity and compliance

tasks [31]. SMEs should assess the factors affecting ownership costs in both short and long terms. The factors can be licensing and subscription fees, implementation costs, training requirements, data migration expenses and maintenance as well as support costs. Choosing a user-friendly design is a strategic decision as it reduces the total cost of ownership and increases return on investment.

SMEs in Finland should explore and take advantages of programs and resources provided by government. These are generally free and specific to Finnish context. Maturity assessment tool such as Kybermittari and financial support provided can be beneficial for organisations to improve their cybersecurity posture. SMEs should also conduct a security due diligence by checking security documents, reports, certifications and data retention policies to ensure secure data handling and processing by vendors. This reduces the risks of introducing new vulnerabilities. Leveraging national support and vetting vendors rigorously forms a proactive and multi layered strategy that strengthens the overall security and compliance significantly for SMEs.

Finally, SMEs should assess user reviews, training resources and document quality of potential solution provider. Assessing customer assistance and account management can be crucial to compensate internal skill gaps making it easier for SMEs to maintain and improve the cybersecurity posture over time. SMEs can ensure that their cybersecurity measures evolve alongside threat landscape and business needs by selecting a vendor that offers robust reliable support. This careful and strategic selection process enables a long-term partnership that protects investment and sustains their security framework effectively.

8.2 For GRC tool vendors

To diminish the market gaps between economically accessible and operationally usable tools for SMEs, vendors and tool developers should focus on developing lightweight, SME-oriented solutions. It is essential for tools to be intuitive and easy to use for small businesses which lack cybersecurity expertise. Vendors should minimise configuration and onboarding burdens by incorporating automation capabilities and pre-built templates for policies, risk registers and compliance mappings. The tools can be more appealing to resource constrained SMEs when the manual setup and deployment time are reduced.

It is crucial for SMEs to get a transparent pricing model that reflects the total cost of ownership. Vendors should clearly communicate costs for ownership, subscription models and other add-

ons costs so that SMEs can make informed decisions without hidden financial commitments. Vendors are recommended to improve the quality of training materials and supporting documents as comprehensive and reliable resources enhance confidence and adoption success. Moreover, an efficient and responsive customer channel with accessible technical support, onboarding assistance can build trust for SMEs.

8.3 For policymakers

It is important for policymakers and national authorities to enhance the effectiveness and accessibility of cybersecurity support for SMEs. The outreach efforts should be increased to ensure awareness of existing subsidies, funding programmes and tools such as Kybermittari. SMEs that are unaware of these resources may limit their ability to implement structured cybersecurity practices. Policymakers should work on simplifying cybersecurity guidance by translating regulatory and framework requirements into clear and SME friendly context. Breaking down technical jargons can attract small businesses to try and adopt cybersecurity practices as a part of their daily operation.

Policymakers and concerned authorities should build a sector-specific compliance roadmaps by addressing unique risks and regulatory expectations found in different industries. This supports SMEs to make an informed decision in implementing security controls and compliance frameworks. Structured guidance programmes tailored to SMEs maturity levels can enable practical adoption of cybersecurity measures. Finally, national authorities should facilitate stronger private-public partnerships to expand accessibility of expert knowledge, training resources and advisory support for SMEs. Collaborative approach can be beneficial for SMEs as it provides access to larger ecosystem of practical assistance.

9 Conclusion

This thesis has investigated the challenges of cybersecurity compliance in Finnish SMEs and the role of scalable GRC tools in addressing them. The evolving landscape of regulatory obligations require SMEs to have a structured governance, risk management and compliance processes to control the impact of sophisticated cyber threats. The structured practices not only ensure smooth day-to-day operations and business continuity during incidents but also enhance customer trusts and build competitive advantage. Adoption of right scalable GRC tool helps to structure the approaches taken for cybersecurity compliance not only by large enterprises but also by small and medium sized enterprises.

It was discovered, limited number of academic research have been conducted on the subject of cybersecurity compliance by SMEs using GRC tools. The research gap indicated that the most of the available security frameworks and solutions focused on large organisations which are often too complex, costly and resource intensive for smaller organisations to implement effectively. This resulted in SMEs perceiving and believing that GRC solutions are fundamentally applicable for larger enterprises and not suitable for their operational realities. The empirical study conducted combining survey data from Finnish SMEs and comparative analysis of tools establishes that the compliance struggle stems from a fundamental misalignment between the capacities of SMEs and available GRC solutions. The findings revealed that resource constraints force SMEs to rely on manual processes which are inadequate for navigating complex regulations and standards ultimately increasing costs and risks. The adopted informal manual and ad hoc processes are ineffective for Finnish SMEs operating in critical sectors under the scope of NIS2 directive that demands a formal risk management and incident reporting requirements.

The scope of the thesis was limited to the SMEs in Finland operating in providing digital services, critical supply chain and the ones handling and processing private information. This limitation narrowed the eligible SME representatives to participate in the survey which resulted in responses from 16 participants. While the result may not represent the vast arena of SMEs, it provides a foundational base for understanding the current state of cybersecurity compliance among SMEs in Finland and their attitude towards adaptation of GRC tools for compliance.

Similar to the existing previous studies, this study indicated SMEs often lack budget, inhouse expertise, resources. These constraints limited SMEs to invest in cybersecurity. The survey

finding illustrated that the SMEs in Finland were generally aware about the global and regional cybersecurity frameworks however, implementation was rather partial or none. The cost associated and complexity of the frameworks were topmost reasons for non-compliance.

Additionally, the SMEs in Finland seemed uncertain about the effectiveness of using GRC solutions as they believed the tools were complex, costly and demanded external manpower for implementation. This indicated that the efforts by GRC vendors to educate small organisations about their product were insufficient and there are not enough solutions in the market that could address the needs of these organisations. Consequently, this perception gap not only hinders adoption but also compels SMEs for manual inefficient compliance practices leaving them exposed to regulatory and security risks.

The thesis incorporates a comparative analysis of four GRC tools available in the market to evaluate how and if they were able to contribute to the requirements of SMEs. The analysis also validated the economical and operational scalability gap as identified in the survey findings. This explained why the SMEs struggle to find effective tools and underscored the necessity for multi-stakeholder recommendations proposed in the thesis. It was noted that bodies like ENISA and NCSC-FI provided guidelines along with financial support targeted to small businesses to improve security posture of their organisations. However, the survey data from participating Finnish SMEs demonstrated that these efforts were not as accessible in terms of awareness. Kybermittari, a free tool for cybersecurity maturity assessment provided by the NCSC-FI was relatively less known by Finnish SMEs. This showcased a need an effective outreach programs by national bodies to encourage structured cybersecurity compliance process.

Based on the results presented by the survey and comparative analysis of GRC tools, some actionable recommendations for SMEs, GRC vendor and policymakers were presented. The SMEs are recommended to adopt a strategic approach rather than reactive while selecting a tool. The vendors are recommended to redesign their products and business models towards implied and SME focused solutions. The policymakers should create mechanisms to translate complex security requirements to SME friendly terms and foster partnerships. Combining simplified, automated GRC processes with supportive policy and education, the Finnish SMEs can progressively improve their compliance posture.

In conclusion, SMEs in Finland can seamlessly improve cybersecurity compliance by adopting an integrated GRC solution despite the challenges. Moreover, closing the gaps require coordinated action across all stakeholders to make GRC solutions accessible and effective for

the Finnish SMEs. The ever-evolving landscapes of technology, threats and regulatory obligations require further studies and research specific to SMEs and their needs.

9.1 Future Research

This thesis provides a comprehensive answer to the raised research questions about the adoption of GRC tools for cybersecurity compliance by SMEs. It also lays a groundwork for further research. There have been limited number of studies in the area thus, future studies could investigate the GRC tool implementation success and return on investment overtime to evaluate effectiveness in real world. Technology evolution and emerging threats demand more attention to protect data, systems and infrastructures. Technology such as AI has been emerging as an integral part of business processes which also exposes SMEs to new cyber risks. Current security standards and frameworks do not explicitly address AI related threats and challenges. Research exploring the adoption of emerging frameworks for AI management in context of SMEs could be conducted.

Further studies in relation to incorporating AI controls and mechanism in GRC tools could be valuable for increasing adoption. Additionally, a comparable study to this thesis that investigates the cybersecurity governance, risk management and compliance challenges faced by SMEs across Europe as well as the role of GRC platforms to mitigate these challenges could be conducted for future research. This could help evaluate the similarities and differences between Finnish SMEs and SMEs in other EU countries to identify cultural and regulatory factors that might affect compliance.

Overall, the thesis demonstrates that transforming cybersecurity compliance from burden to advantage requires coordinated actions across the whole ecosystem of SMEs, vendors and policymakers. SMEs must adopt to strategic procurement practices; vendors must lean towards scalability and small businesses focused while policymakers must create enabling conditions for platform adoption. It is necessary to understand that the journey towards compliance is not just technical but organisational and economical. Finnish SMEs can build compliance and resilience while turning regulatory requirements to strategic advantage securely by addressing the misalignment between needs and solution identified in the thesis.

References

[1] "Entrepreneurship in Finland," Yrittäjät, 2023. [Online]. Available: https://www.yrittajat.fi/en/about-us/information-about-yrittajat/entrepreneurship-in-finland/. [Accessed 20 August 2025].

[2] H. Uitto, K. Halme, V. Salminen and T. Kotilainen, "Impact evaluation of the financial support provided by the National Coordination Centre Finland (NCC-FI)," Finnish Transport and Communications Agency Traficom, 2025. Available: https://www.traficom.fi/sites/default/files/media/publication/Impact%20evaluation%20of%20the%20financial%20support%20provided%20by%20the%20National%20Coordination%20Centre%20Finland%20%28NCC-FI%29.pdf.

[3] E. European Union Agency for Cybersecurity, "Cybersecurity for SMEs, Challenges and Recommendations," ENISA, 2021.Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf.

[4] A. Renvall, "Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs," Helsinki Metropolia University of Applied Sciences, Helsinki, Finland, 2018.Available: https://www.theseus.fi/bitstream/handle/10024/157277/Renvall_Aleksi_final.pdf.

[5] N. Racz, E. Weippl and A. Seufert, "A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)," in Communications and Multimedia Security (CMS 2010), Lecture Notes in Computer Science, vol.6109, Berlin, Heidelberg, Germany, 2010, doi: https://doi.org/10.1007/978-3-642-13241-4_11.

[6] M. V. Karthick, D. J. Prabhakaran, M. P. Banu and D. U. Senthil Kumar, "Systematic Literature Review on GRC - A Study on Best Practices and Implementation Strategy in GRC," Samdarshi, vol. 16, no. 4, 2023. Available: https://www.researchgate.net/publication/381488401_Systematic_Literature_Review_on_GRC_-A_Study_on_Best_Practices_and_Implementation_Strategy_in_GRC.

[7] S. Savaş and S. Karataş, "Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance," International Cybersecurity Law Review, vol. 3, pp. 7-34, 2022, doi: https://doi.org/10.1365/s43439-021-00045-4.

[8] C. Gilbert and M. A. Gilbert, "Cybersecurity Risk Management Frameworks for Critical Infrastructure Protection," International Journal of Research Publication and Reviews,

vol. 5, no. 12, pp. 507-533, 2024. Available: https://www.academia.edu/126048402/Cybersecurity_Risk_Management_Frameworks_for_Critical_Infrastructure_Protection?email_work_card=view-paper.

[9] G. O. Babatunde, A. A. Alabi, S. D. Mustapha and A. B. Ige, "A Governance, Risk, and Compliance (GRC) Model to Simplify Regulatory Compliance for North American Businesses," IRE Journals, vol. 6, no. 11, pp. 917-935, 2023. Available: https://www.irejournals.com/paper-details/1704406.

[10] M. Syafrizal, S. R. Selamat and N. A. Zakaria, "Analysis of Cybersecurity Standard and Framework Components," International Journal of Communication Networks and Information Security (IJCNIS), vol. 12, no. 3, pp. 417-428, 2020.doi: https://doi.org/10.17762/ijcnis.v12i3.4817.

[11] S. S. Marhad, S. Z. A. Goni and M. K. J. Abdullah Sani, "Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review," in 2nd International Conference on Information Science, Technology, Management, Humanities, and Business, Shah Alam, Malaysia, 2023, doi: https://doi.org/10.21834/e-bpj.v9iSI18.5483.

[12] S. Chavez, J. Anahue and W. Ticona, "Implementation of an ISMS Based on ISO/IEC 27001:2022 to Improve Information Security in the Internet Services Sector," in International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2024, doi: https://doi.org/10.1109/confluence60223.2024.10463392.

[13] A. Folorunso, V. Mohammed, I. Wada and B. Samuel, "The impact of ISO security standards on enhancing cybersecurity posture inorganizations," World Journal of Advanced Research and Reviews, vol. 1, pp. 2582-2595, 2024, doi: https://doi.org/10.30574/wjarr.2024.24.1.3169.

[14] ENISA, "Network and Information Systems Directive 2 (NIS2)," ENISA, [Online]. Available: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2. [Accessed 5 September 2025].

[15] European Parliament and Council, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E," Official Journal of the European Union, no. L 333, pp. 80-152, 2022. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022L2555.

[16] S. D. Haes, W. V. Grembergen and R. S. Debreceny, “COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities,” Journal of Information Systems, vol. 27, no. 1, pp. 307-324, 2013, doi: https://doi.org/10.2308/isys-50422.

[17] ISACA, “COBIT 2019 framework: introduction & methodology,” 2019. [Online]. Available: https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf. [Accessed 8 September 2025].

[18] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” 26 February 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. [Accessed 8 September 2025].

[19] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Accessed 8 September 2025].

[20] Center for Internet Security, “CIS Controls Version 8,” May 2021. [Online]. Available: https://kr-labs.com.ua/books/CIS_Controls_v8_Guide.pdf. [Accessed 9 September 2025].

[21] Kyberturvallisuuskeskus, “Kybermittari - Cybermeter,” National Cyber Security Centre Finland, Finnish Transport and Communications Agency Traficom, 11 October 2024. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter. [Accessed 10 September 2025].

[22] Kyberturvallisuuskeskus, “Cybermeter, National framework for the assessment of cybersecurity capabilities, User guide,” [Online]. Available: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_Cybermeter_User_Guide_V1.pdf. [Accessed 10 September 2025].

[23] S. Muthaiyah and T. O. K. Zaw, “ISO/IEC 27001 Implementation in SMEs: Investigation on Management of Information Assets,” Indian Journal of Public Health Research & Development, vol. 9, no. 12, 2018. doi: https://doi.org/10.5958/0976-5506.2018.02112.5.

[24] M. Antunes, M. Maximiano, R. Gomes and D. Pinto, “Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal,” Journal of

Cybersecurity and Privacy, vol. 1, no. 2, pp. 219-238, 2021, doi: https://doi.org/10.3390/jcp1020012.

[25] D. R. Ejjami, "Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives," Journal of Next-Generation Research 5.0, 2024. Available: https://jngr5.com/index.php/journal-of-next-generation-resea/article/view/99/71.

[26] E. Kaiser, "The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations," Journal of media law, vol. 1, 2023. Available: https://www.medialaws.eu/rivista/the-new-nis-ii-directive-and-its-impact-on-small-and-medium-enterprises-smes-initial-considerations/.

[27] H. C. C. da Silva, D. S. da Silveira, J. S. Dornelas and H. S. Ferreira, "Information technology governance in small and medium enterprises - a systematic mapping," Journal of Information Systems and Technology, vol. 17, no. 1-16, 2020, doi: https://doi.org/10.4301/S1807-1775202017001.

[28] National Institute of Standards and Technology, "NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide Overview," February 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf. [Accessed 11 September 2025].

[29] H. Mehta, "Managing Cyberrisk with the Help of GRC," 9 October 2024. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2024/volume-5/managing-cyberrisk-with-the-help-of-grc. [Accessed 18 September 2025].

[30] M. O. Faruq, "A meta-analysis of cybersecurity framework integration in GRC platforms: evidence from U.S. enterprise audits," Journal of Sustainable Development and Policy, vol. 1, no. 1, pp. 224-249, 2025, doi: https://doi.org/10.63125/kwhkmb57.

[31] European union agency for cybersecurity, "Cybersecurity guide for SMEs," [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Cybersecurity%20guide%20for%20SMEs-online-single_page.pdf. [Accessed 22 September 2025].

[32] E. Guttman and N. Brownlee, "Expectations for computer security incident response," RFC 2350, BCP 21, Internet engineering task force, June. 1998. doi: https://doi.org/10.17487/RFC2350.

[33] C. Steglich, I. Poltronieri and A. F. Zorzo, "Mind the Gaps: An Infosec Grc Roadmap Research for Small Organisations," SSRN, 2025, doi: https://dx.doi.org/10.2139/ssrn.5384356.

[34] F. Morten, O. Henning, E. S. Knud, T. Reza and W. Idongesit, “Cybersecurity Strategies for SMEs in the Nordic Baltic Region,” Journal of Cyber Security and Mobility, vol. 11, no. 6, pp. 727-753, 2022, doi: https://doi.org/10.13052/jcsm2245-1439.1161.

[35] C. Ponsard and J. Grandclaudon, “Guidelines and Tool Support for Building a Cybersecurity Awareness Program for SMEs,” in International Conference on Information Systems Security and Privacy, Prague, Czech, 2019, doi: https://doi.org/10.1007/978-3-030-49443-8_16.

[36] T. Sendjaja, Irwandi, E. Prastiawan, Y. Suryani and E. Fatmawati, “Cybersecurity in The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks,” International Journal of Science and Society (IJSOC), vol. 6, no. 1, 2024, doi: https://doi.org/10.54783/ijsoc.v6i1.1098.

[37] A. Marotta and M. Staurt, “Analyzing the Interplay Between Regulatory Compliance and Cybersecurity,” SSRN Electronic Journal, 2020, doi: https://dx.doi.org/10.2139/ssrn.3569902.

[38] S. Pawar and H. Palivela, “Need of Paradigm Shift in Cybersecurity Implementation for Small and Medium Enterprises (SMES),” International Journal of Cybersecurity Intelligence and Cybercrime, vol. 8, no. 1, pp. 39-75, 2025, doi: https://doi.org/10.52306/2578-3289.1184.

[39] A. L. Mitrofan, E.-V. Cruceru and A. Barbu, “Determining the main causes that lead to cybersecurity risks in SMEs,” Business Excellence and Management, vol. 10, no. 4, pp. 38-48, 2020. Available: https://paperity.org/p/261851955/determining-the-main-causes-that-lead-to-cybersecurity-risks-in-smes.

[40] B. Lill, C. Sauerwein, A. Zeisler, C. Hochstrasser and N. Mexis, “Assessing Cybersecurity Readiness Among SME,” in International Conference on Enterprise Information Systems, Lisboa, Portugal, 2025, doi: https://doi.org/10.5220/0013353400003929.

[41] A. Adebayo, M. A. Moronkunbi, O. C. Oyedeji, S. A. Samuel and P. O. Victor, “The Role of IT Governance Risk and Compliance (IT GRC) in Modern Organizations,” International Journal of Latest Technology in Engineering Management & Applied Science, vol. XIII, no. VI, pp. 44-50, 2024, doi: https://doi.org/10.51583/IJLTEMAS.2024.130607.

[42] O. I. Enitan, “Enhancing Cybersecurity Readiness in SMEs: Addressing Resource Constraints and Policy Gaps through Scalable Solutions and IT Investments,” International Journal of Multidisciplinary in Cryptology and Information Security, vol. 14, no. 1, 2025, doi: https://doi.org/10.30534/ijmcis/2025/011412025.

[43] O. Ogunjimi, A. Alfolorunso and O. Olukomoro, “Elicitation of SME Requirements for Cybersecurity Solutions Through Adherence to Recommendations,” Advances in Mathematical & Computational Sciences, vol. 6, no. 2, pp. 29-34, 2018. doi: https://doi.org/10.22624/AIMS/MATHS/V6N2P4.

[44] S. Vitla, “Enhancing Cybersecurity Compliance through Identity Governance Solutions,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology IJSRCSEIT, vol. 10, no. 1, pp. 277-293, 2024. Available: https://www.academia.edu/126983123/Enhancing_Cybersecurity_Compliance_through_Identity_Governance_Solutions.

[45] R. Paananen, M. Soikkeli, M. Starck, M. Aro, T. Kuusisto and T. Tuulensuu, “Finland’s Cyber Security Strategy 2024–2035,” Prime Minister’s Office, Government of Finland, Helsinki, 2024. Available: https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/content.

[46] L. Mangold, “OpenGRC Documentation,” OpenGRC, [Online]. Available: https://docs.opengrc.com/. [Accessed 2 October 2025].

[47] Eramba Forum, “Eramba: Governance, risk and compliance platform,” Eramba, [Online]. Available: https://discussions.eramba.org/latest. [Accessed 2 October 2025].

[48] Sprinto, “SMB compliance solutions,” Sprinto, [Online]. Available: https://sprinto.com/blog/. [Accessed 3 October 2025].

[49] Cyberday, “Cybersecurity and compliance automation for SMEs,” Cyberday Inc, [Online]. Available: https://www.cyberday.ai/. [Accessed 5 October 2025].

[50] O. Abdul-Azeez, A. O. Ihechere and C. Idemudia, “Digital access and inclusion for SMEs in the financial services industry through Cybersecurity GRC: A pathway to safer digital ecosystems,” Finance & Accounting Research Journal, vol. 6, no. 1, pp. 1134-1156, 2024, doi: https://doi.org/10.51594/farj.v6i7.1270.

Appendix

Survey Questionnaire: Cybersecurity Compliance in Finnish SMEs

This survey aims to explore the challenges, tools, and practices influencing cybersecurity compliance among Small and Medium-sized Enterprises (SMEs) in Finland. The focus is on organizations processing personal data, providing digital services, or operating in critical supply chains.

Section 1: General Information

(Purpose: To understand the context of the organization)

1. What is your organization's size (number of employees)?

o 1–9

o 10–49

o 50–249

2. Which sector best describes your organization's primary operations?

o Information and Communications Technology (ICT) / Digital Service

o Finance / Insurance / Professional Services

o Manufacturing / Industrial Production

o Energy / Utilities / Critical Infrastructure

o Healthcare / Social Services

o Other (please specify): _____

3. What is your current role in the organization?

o CEO / Founder

o IT / Security Manager

o CISO / Compliance / Risk Officer

o Other (please specify): _____

4. Do you have a dedicated cybersecurity or IT compliance function within your organization?

o Yes

o No

o Outsourced

Section 2: Current Cybersecurity & Compliance Practices

(Purpose: To explore the current approach to cybersecurity compliance)

5. Are you familiar with any of the following cybersecurity or compliance frameworks? (Select all that apply)

o ISO/IEC 27001

o NIS2 Directive

o GDPR

o NIST Cybersecurity Framework

o COBIT

o CIS Controls

o Kybermittari (Cybermeter)

o None

6. Has your organization implemented any of the above frameworks?

o Fully implemented

o Partially implemented

o Planning to implement

o Not implemented

7. How does your company currently manage its cybersecurity compliance

activities? (Select all that apply)

o Dedicated GRC or compliance software

o Spreadsheets (e.g., Excel, Google Sheets)

o Documents (e.g., Word, Google Docs)

o Manual processes and ad-hoc checks

o External consultants

o We do not have a formalized process.

o Other: _____

8. Which of the following challenges most affect your organization's cybersecurity compliance? *(Select up to 3)*

o Budget constraints

o Lack of expertise

o Lack of management support

o Complexity of frameworks

o Limited staff time

o Unclear regulatory requirements

o Other: _____

Section 3: Governance, Risk, and Compliance (GRC) Tools Adoption

(Purpose: To understand potential reasons to adopt or not adopt a GRC tool)

9. Does your organization currently use a GRC tool or software to manage cybersecurity compliance?

o Yes

o No

o Not sure

10. If yes, which GRC tool do you use?

o Open-source tool

o Commercial tool

o In-house developed tool

11. How effective do you find your current GRC tool in supporting compliance activities?

o Very effective

o Moderately effective

o Slightly effective

o Not effective

12. What key features would you expect from an ideal GRC tool designed for SMEs? (Select all that apply)

o Easy-to-use interface

o Automated compliance reporting

o Integration with existing systems

o Risk scoring and dashboards

o Affordable cost

o Support for Finnish/European regulations

o Other: _____

Section 4: Perceptions and Future Intentions

(Purpose: To understand SME attitude toward compliance improvement)

13. How would you rate your organization's overall cybersecurity maturity level?

o Low

o Moderate

o High

o Very high

14. How likely is your organization to invest in cybersecurity frameworks or tools within the next 12 months?

o Very likely

o Somewhat likely

o Neutral

o Unlikely

15. What support would be most helpful in improving cybersecurity compliance? (Select all that apply)

o Training and awareness

o Financial assistance/subsidies

o Sector-specific guidance

o Access to simple and scalable tools

o Expert consultancy

o Other: _____

Thank you for participating in this survey. Your input will contribute to understanding the current state of cybersecurity compliance among Finnish SMEs and support the development of more effective GRC solutions.