jamk

Qualitative evaluation of attributes Influencing information security setup in SME organization

Priyanka Das Bokalial

Master's thesis
May 2025
Master's Degree Programme in Information Technology, Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Das Bokalial Priyanka

Qualitative evaluation of attributes Influencing information security setup in SME organization

Jyväskylä: Jamk University of Applied Sciences, May 2025, 49pages.

Degree Programme in Information Technology, Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

Irrespective of any industry the information security SME companies need to implement various ISMS standards needed to maintain the ISO standards by a company from small sized company to medium sized company. Earlier it was easier to ignore but with GDPR, COVID and Modern warfare, it has become very important that the SME companies understand the importance of cybersecurity and based on that make decision what and how to protect the company's assets in the new digital threat landscape.

A minimal feasible security framework should be created, which is important for business processes and will make its employees, customers and suppliers aware of the technological threats and how to safeguard and protect the company with minimal security instead of thinking of very complex security structure. The thesis uses systematic review with mixed method which contain both qualitative and quantitative methods by using evaluating the survey answers shared with few SME companies and the articles from the databases.

With the business growth and profitability, the number of employees in the company also grows, so it's very important to implement ISMS inorder to protect company's sensitive data, reputation and customer's trust and should create a security framework for the company so that if any security incident happens, then instead of panicking it should stick to its security framework and take the necessary actions which are needed to handle the security incident. This can be achieved by referring to ISO 27002:2022 which provides detailed information and advice on why some of the security controls are required. The step-by-step guidance provided by ISO 27002 can help the SMEs to plan out the ISMS implementation for all the critical assets and abide by the various data privacy policies and security compliant requirements.

Keywords/tags (subjects)

SME, ISO 27002:2022, training, growth, GDPR, ISMS

Miscellaneous (Confidential information)

N/A

Contents

Figures

Tables

1 Introduction

Information Security Management Systems (ISMS) are very crucial for SMEs from the foundation itself. With the rise in digital threats and implementation of various regulations, all the companies irrespective of any industry from startup to medium sized should understand the importance of cyber security and start to implement the bare minimum cybersecurity framework to protect all the company's assets. This can be very clearly understood when the team refers to ISO 27002:2022 documentation, which is extensive but will help to get a rise from small topics based on organizational, people, physical and technological controls (Harvey, 2024). Receiving advice from different sources creates lots of confusion, so SME-ISC guide which provides clear and simple control guidance will help the SMEs to implement cybersecurity properly (Renaud, 2016). In the thesis, it's highlighted that the minimal security framework should be implemented to bring in more customers and increase their trust which will lead to the growth of business. With the basic information security policy implementation, the company grows and with time the infosec understanding also deepens and as a result, in future more detailed and extensive security framework can be explored and implemented (Kaila, 2018).

In this thesis, there are 5 different chapters. In chapter 2, I have put in my research methodology used to complete my thesis work. Then chapter 3 explains the theory part about why it's important for SMEs to implement and improve their Information security posture to make their business stable and grow by referring to ISO 27002:2022 and various books, journals and blogs. In Chapter 4, the survey is discussed with the answers provided by companies and has also put together my point of view about the different topics. Chapters 5 and 6 provides the conclusion and discussion about the survey and importance of implementing Information security by SMEs.

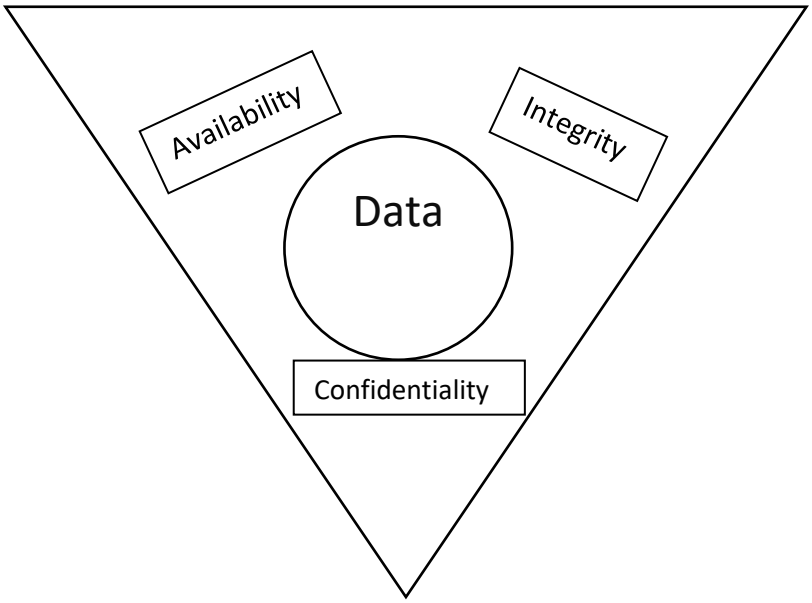


Figure 1: CIA triad

2 Research methodology

2.1 Research Question

Main research question which was the objective of the study:

How implementing information security policies with the help of ISO 27002:2022 would help in strengthening the foundation of information security in an SME company?

And the additional research questions which were a part of the survey are:

1. How data protection plays a major role in implementing information security.
2. Does having a strong foundation in information security and data privacy lead to growth in business and gain customers trust?

2.2 Research method

In this research method, survey answers are used to study the information security knowledge and the posture an SME company should have before. It combines both the qualitative and

quantitative methods to provide more comprehensive systematic understanding about how information security can be implemented in an SME company (Dovetail Editorial Team, 2023).

Initially the study was planned to start with qualitative research methods, but while identifying and understanding the research questions and what the main goal is, it was identified that I should go with mixed method with systematic review. The table below explains the difference between qualitative and quantitative research methods (Streefkerk, 2019).

Table 1: Difference between qualitative and quantitative research methods

Data collection method	**Qualitative research method**	**Quantitative research method**
Focus	Exploring ideas	-
Analysis	Summarizing, categorizing, interpreting	-
Expressed in	Words	Yes or No
Sample	Few respondents	-
Questions	-	Survey with multiple choice options
Characterized by	Understanding	-

Below are my survey questions and details are explained in chapters 3 and 4:

SQ7. Does your organization have its own documents and policies so that the employees can comply with the information security standards in order to prevent data breaches of sensitive and confidential information?

SQ8. Are the security policies at your organization reviewed and updated at regular intervals?

SQ9. Are the documented security policies at your organization easily accessible and understandable by the employees?

SQ10. Does your company have its own IT security training materials available for the employees to ensure that they know how to handle sensitive information?

SQ11. Are the GDPR guidelines at your organization followed while handling your clients/customers data?

SQ12. Where are your organization's data stored?

SQ13. Is the multi-factor Authenticator (MFA) enabled for all/part of the softwares used in your organization?

SQ14. When using any software for work purpose is it's security policy reviewed for GDPR purpose like where your organization 's data will be stored and what information will it gather?

SQ15. Do you organization have any automated way of obtaining the software Inventory if you are working globally?

SQ16. Does the antivirus software installed in your organization 's devices have malware protection capability?

SQ17. Are the endpoints or laptops provided by your organization encrypted?

SQ18. Are there any processes to handle the patches to take care of the various vulnerabilities where the critical security updates are managed centrally?

SQ19. Do your organization provide any remote working tool for secure remote access?

SQ20. Are there any business continuity plans documented and implemented for your organization?

The survey questions in Appendix 1 start with qualitative data collection and analysis and then based on that it led to quantitative data collection and analysis interpretation to understand more from the findings (Harvard Catalyst, 2022).

Both qualitative and quantitative study leads to traditional epidemiological study, which helps to prepare for and minimize the disaster and prevent business disruptions in any kind of cybersecurity incidents (Modini et al., 2020).

2.2.1 Qualitative research method

Qualitative research method provides an in-depth and contextual understanding of the project outcomes and participant experiences which emphasizes the importance of the evaluation and helps in exploring the issues by explaining the 'why' and 'how' logic behind the project outcomes (TolaData, 2021). It helps in demonstrating the practical value in real world settings.

Qualitative methods like interviews and focus groups offer insights into participant experiences, providing a deeper understanding of program impacts (TolaData, 2021).

2.2.2 Quantitative research method

Quantitative methods give a general understanding which makes data easier to collect and study precisely by using surveys, questionnaires, and numerical data to measure progress and outcomes (TolaData, 2021).

2.2.3 Mixed Research method

Mixed data collection method explains the integration approach of both qualitative and quantitative data collection methods to provide a comprehensive understanding of research questions (Chegg Writing, 2021).

One of the mixed methods is **convergent parallel mixed method**, where both types of qualitative and quantitative data are collected simultaneously and are compared and interpreted together to draw some meaningful conclusions and is shown in the figure below (Chegg Writing, 2021).

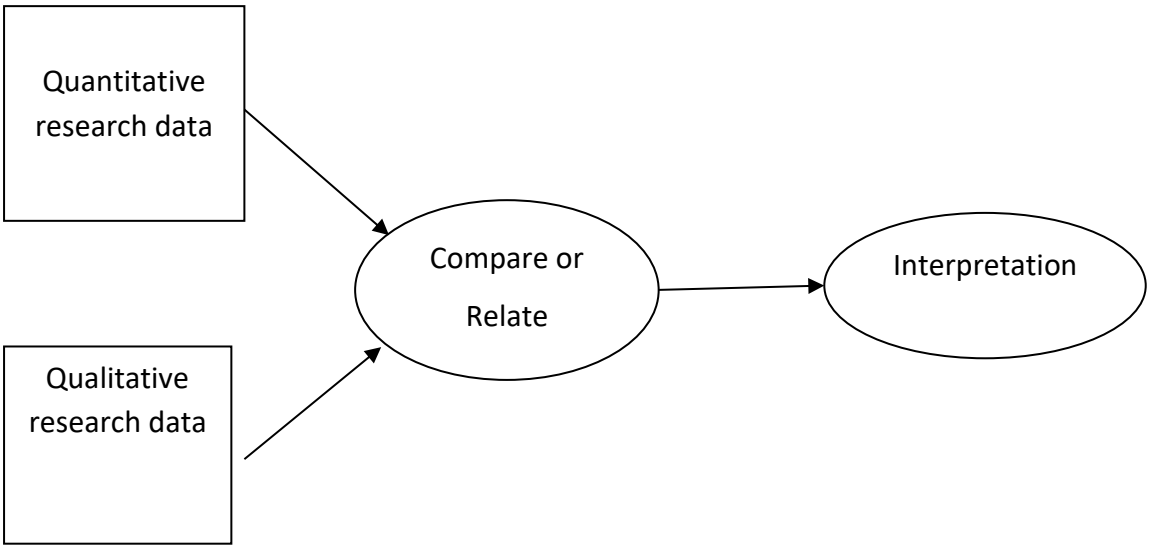


Figure 2: Convergent parallel mixed method (Chegg Writing, 2021)

2.2.4 Data collection and Analysis method

The survey questions were categorized into a few different topics: security policy, accessibility of documents, data storage, software usage, laptop security, and business continuity plan. Then based on that, systematic review is conducted to perform the research. Various journals were referred to by Google Scholar, ResearchGate, ScienceDirect and ProQuest Ebook Central was used to refer to few books. The systematic review was opted later as the survey answers were very limited due to non-availability of non-disclosure agreement (NDA) with the respondent companies making it more challenging as there were privacy and confidentiality concerns, as the survey holds some sensitive topics about the workplace. And there might be some legal issues and trust issues as companies wouldn't want to share their IT related matters to any outsiders without the NDA. Moreover, the research was restricted to only Finland, which limited the participants numbers and sometimes it's hard to verify if the answers provided in the survey are accurate and even implemented in the company. Therefore, the systematic review was conducted to perform my research. In the figure below, there is a systematic search process for the selection of articles using PRISMA flow diagram (Pandey et al., 2022).

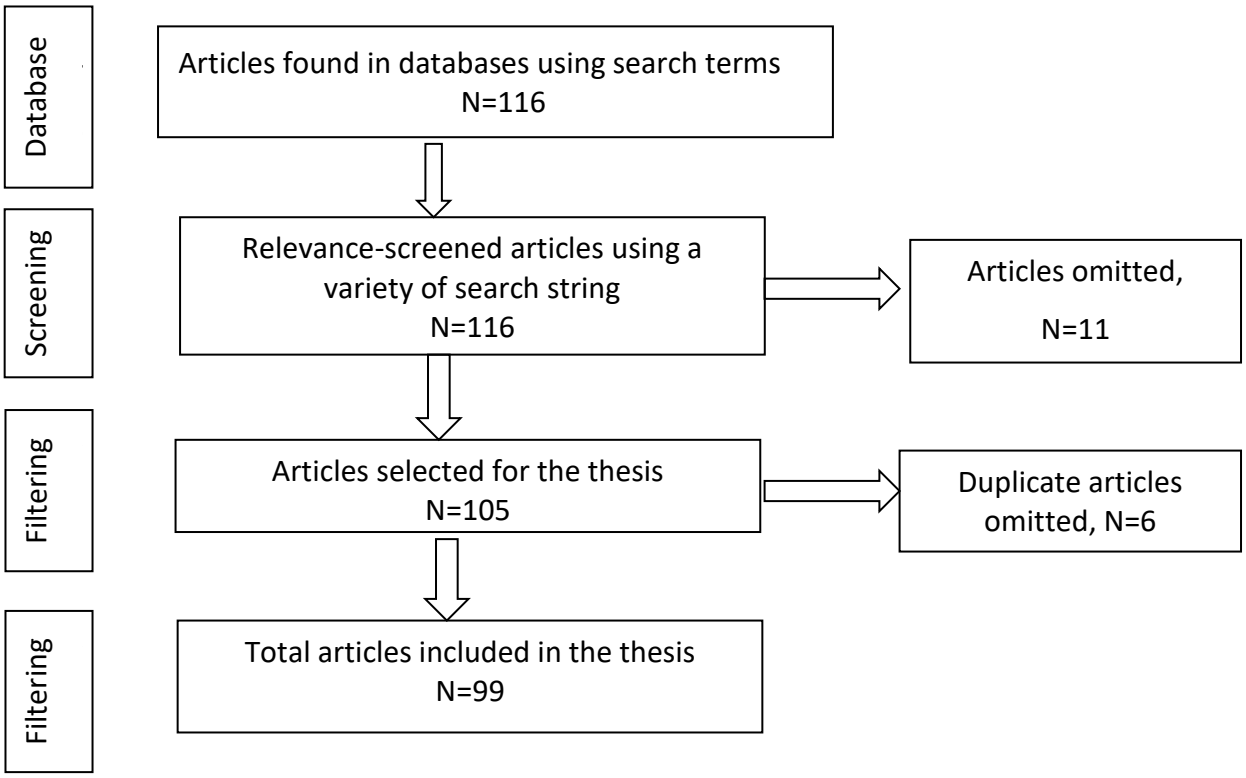


Figure 3: PRISMA flow diagram for Systemmatic review

2.3 Research ethics and reliability

The research for this thesis has followed the ethical recommendations mentioned in the Ethical Principles of JAMK University of Applied Sciences and follows the Finnish Code of Conduct for Research Integrity and Procedures for Handling Alleged Violations of Research Integrity in Finland,2023. The research and the survey data were collected with honesty and for any personal data that includes the respondents names and e-mail IDs, and the survey answers are kept secured in accordance with GDPR.

JAMK's official survey tool 'Webropol' was used to collect the survey data and all the reference materials like books, journals and blogs are obtained from legitimate sites according to the reporting instructions of Yampa.

To lead me to my referenced links Google Scholar, ProQuest Ebook Central, ResearchGate and ScienceDirect was used which helped me to gain knowledge while writing the thesis. Perplexity AI helped me in finding out some relevant latest security articles and journals.

2.4 Previous research

According to the previous research by Siitonen (2020), it studied the risk management part of Finnish SMEs, where it was identified that the risk management process is often inconsistent, which is always in a developmental situation and is usually managed by only the IT manager. The study emphasizes more about the different consistent processes involved in risk management process according to ISO 31000 standard. Interviews were conducted where the different challenges about risk management were discussed and how it could be also improved in the SMEs in a systematic way.

According to the previous research by Bråthen & Lie (2021), it conducted a cyber security awareness survey in SME's through qualitative and mixed research method and a literature review. According to the survey conducted, all the employees in an SME company need to be aware of the different cybersecurity implementations in all business-related activities and they should follow the organization's information security rules and regulations, although the employees claim that they are aware and understand about cybersecurity. In this thesis it uses the concept of Meaning, Behavior, and Knowledge which are important parts of cybersecurity awareness literature.

According to the previous research by Renvall (2018), it emphasized the use of ISO 27001 information security standard to enhance the cyber security infrastructure of SMEs. The author has investigated that threats, incidents and vulnerabilities are all interrelated and explained about the different cybersecurity threats, EU’s GDPR, ISO/IEC 27001 and other information security standards and how adoption of any of these standards help to improve the cybersecurity of SME companies.

According to the previous research by Laine (2024), it explained how the development environment of an SME company can be improved to obtain the ISO 27001 certification by implementing the different best practices of DevOps. A part of the thesis includes the cyber security

posture study of a company where it also checked for opportunities associated with open-source intelligence.

According to the previous research by Flyktman (2016), it mentioned the OODA loop which has many dimensions and can help in organizing the operations of information security. It discusses the different views of information security by the public regarding the data breach and the cost involved with it. It explains why information security is not implemented properly although the SME companies are committed to it. Apart from identifying the shortcomings, it also mentions how strong information security can be achieved by implementing ISMS strongly. For proper implementation of ISMS, proper Standard Operating Procedure (SOP) should be set up, which is a continuous process and should be done efficiently.

And my research topic relates to initial guidance of how SME's can improve their information security requirements by referring to ISO 27002:2022 which guides how information security should be implemented. I planned my thesis during the COVID times as there were many phishing, malware and ransomware attacks. With remote working at that time, many SME companies had to change their working methods where earlier some companies already had the remote working culture, and some had the office working culture irrespective of any industry. But with the remote work, it brought in enormous amount of cyber security threats. So, I selected a few basic topics where the security settings can be improved in an SME organization by referring to ISO 27002, by using survey and systematic literature approach. The main purpose of choosing ISO 27002 is to understand its importance when the SME company grows and provides their consultancy services to their respective customers. Improving the infosec posture of an SME company is a continuous process, and its development and awareness should always be prioritized. The topics chosen in the survey are basic, which is normally used in daily business but due to cost and delayed plans, much time is not invested in setting up the security area of the cloud, apps and hardware assets. Therefore, it has become the necessity for them to maintain a good cyber hygiene to secure their business by providing:

- Proper cyber security awareness and training.
- Improving the security of all the current assets.
- Proper planning and investing in security softwares.

3 Theory

3.1 SME's

3.1.1 Who are considered

SME enterprises which have less than 250 employees have a turnover of €50 million of economy annually (Flanders innovation & entrepreneurship, n.d). Companies with less than 10 employees are micro-sized companies, with less than 50 employees are small-sized companies and with 50-250 employees are medium-sized companies (European Commission, 2020). The table below shows who are considered SMEs based on employees head count and annual turnover.

Table 2: EU micro-, small- and medium-sized enterprises (European Commission, 2020)

Enterprise category	**Headcount: annual work unit (AWU)**	**Annual turnover**
Medium-sized	< 250	≤EUR 50 million
Small	< 50	≤EUR 10 million
Micro	< 10	≤EUR 2 million

SME's play an important role in the EU economy, which accounts to 94% of the business as recorded in 2023, and contributes to the employment and value added across all the 27 EU member states (European Commission, 2024). Therefore, to protect the EU's economy, it is very important to protect the SMEs from various kinds of cyber-attacks.

Many SME's always aim for their business to grow, which requires proper strategy and investment under any circumstances where with economic changes there's also changes in technology (Levy & Powell, 2004, pg. 23-29). Therefore, investment in information systems succeeds in

two ways, as a low-cost investment or as a value added in strategy (Levy & Powell, 2004, pg 35-50). They can take bank loans and funds from investors to navigate challenges and avoid financial issues (Karaoulanis, 2020, pg. 66).

ENISA helps SMEs to improve their cyber security posture and to secure their business operations by analyzing how it can defend the different cyber threats and by providing various tools, methods, risk assessments, business continuity and cloud and data security (ENISA, 2024).

ENISA, the European Union Agency for Cybersecurity composes of EU Member States representatives, the EU Commission and other stakeholders, and it plays a very crucial role in making Europe cyber secure since 2004 (Agency for Innovation & Entrepreneurship, n.d).

Owners and staff in SMS often lack information security skills, therefore, ISMS implementation can be outsourced to any security consultancy firms, according to the business needs (Critical Risk Solution, 2024).
In the world of digitalization, digital transformation is adopted by many SMEs for business growth and therefore to protect the business from various cyber threats, information security should be implemented properly (Clemente-Almendros et al., 2024).

3.1.2 Importance of Information Security for SME's

To improve the cybersecurity posture of SMEs, Small Business Standards (SBS) in collaboration of European Digital SME Alliance have created an SME guide for implementation of ISO 27001 on various information security management controls (European DIGITAL SME Alliance, 2018). In 2019, the cloud computing market was growing rapidly, and as it was cost efficient, SMEs contributed a lot to the EU's economic growth (Haucap et al., 2022). As a result, access to the latest applications brought in more innovations and focuses in core business and flexible working culture for employees.

It's the responsibility of the management team to make the company cyber resilient by ensuring information security is in place by implementing Information Security Management System

(ISMS) which takes care of information security policies and procedures, asset management, access control management and incident management (European DIGITAL SME Alliance, 2018).

Limited budgets and lack of technical expertise are few of the common IT challenges faced by SMEs, but with detailed security plan and with multiple policies within it, a small company can start building its own ISMS to protect the business and its reputation (Fastech Solutions, 2021). And during the initial phase, as it might be overwhelming and difficult to create the right program, an SME can approach a Managed Service Provider (MSP) who can assess and evaluate different IT solutions and propose a solution according to the company's need considering their future expansion as well (Fastech Solutions, 2024).

3.1.3 Financial impact to consider Information Security/Factors affecting implementation of Information Security by SMEs

During COVID-19 pandemic, low security budget, unskilled cyber skills and rising number of cyber threats, made ENISA take proper steps to help securing SME's businesses (ENISA, 2024).

Although the SMEs are aware of and understand the importance of information security implementation, the main issue is that many doubt, how much worth of investment is needed. By identifying the amount needed to be invested, implementing the right security tools and providing specialized security training to the IT team, information security and monitoring can be implemented (European DIGITAL SME Alliance, 2018). Instead of spending money on costlier tools, investments should be initially done on simple solutions, which help in achieving the business goals but is never a long-term solution (Cheek, 2024, pg 40-44).

Information security blueprint, framework or architecture serves as a vision and the master plan of a cybersecurity program (Schreider, 2019, pg 20-21).

Initially, when there is a shortage in skilled resources due to financial and other reasons, it's always best to outsource to a freelancer or contractor which helps in completing the project timeline without hiring a full-time resource (Cheek, 2024, pg 163).

But as business grows, both in-house and full-time resources can be hired which helps to adapt seamless information sharing within the team and maintain the momentum while recruiting the right team (Cheek, 2024, pg 164).

3.2 ISO 27002:2022

ISO 27002 gives a practical understanding of implementing information security in an SME effectively by understanding the best practices which are needed to implement and improving its security posture providing detailed guidance on how and why to implement the security controls (Delev, 2023).

Although ISO 27002 cannot be certified, it can be used as a reference to implement and prepare an SME company to understand the importance of investing in information security. And once the information security is set up in the early stage of when the company is growing, then it helps in preparing the organization towards the ISO 27001 certification.

ISO 27002 helps SME companies with detailed guidelines for each task, and it breaks down the controls and tasks for managers by reducing the guesswork in ISMS implementation and making it easier to earn 27001 certification (DataGuard, 2023).

Organizations should first assess the different requirements to identify the different possible controls and plan to implement them systematically as recommended and continuously try to improve the different controls.

3.2.1 Implementation of Information Security by SME's after 2020

Based on ISO 27002, a group of experts from Small Business Standards (SBS) and digital SME have selected 16 minimum controls out of 114 controls for protecting and increasing the cyber resilience of the SMEs and ensuring the GDPR compliance (European Digital SME Alliance, 2022). In the table below I have tried to relate my survey questions with controls in ISO 27002 and with the Information Security controls set by European Digital SME and the questions are categorized into different topics: Security policy, Accessibility of documents, Data privacy, Software usage, Laptop security and Business continuity.

Table 3: Establishing relation between my survey, ISO 27002 and Information Security controls set by European Digital SME

Categorization	**Survey questions**		**ISO 27002:2022**	**Controls**
Security Policy	SQ7.	Does your organization have its own documents and policies so that the employees can comply with the information security standards in order to prevent data breaches of sensitive and confidential information?	5.1	2
	SQ8.	Are the security policies at your organization reviewed and updated at regular intervals?	5.1	2
Accessibility of documents	SQ9.	Are the documented security policies at your organization easily accessible and understandable by the employees?	5.1	2
	SQ10.	Does your company have its own IT security training materials available for the employees to ensure that they know how to handle sensitive information?	6.3	13
Data privacy	SQ11.	Are the GDPR guidelines at your organization followed while handling your clients/customers data?	5.19, 5.20, 5.21, 5.22	14
	SQ12.	Where are your organization 's data stored?	5.33, 8.13	8
Software usage	SQ13.	Is the multi-factor Authenticator (MFA) enabled for all/part of the softwares used in your organization?	8.5	4
	SQ14.	When using any software for work purpose is it's security policy reviewed for GDPR purpose like where your organization 's data will be stored and what information will it gather?	5.32	4
	SQ15.	Do you organization have any automated way of obtaining the software Inventory if you are working globally?	8.8, 5.9	1, 6

	SQ18.	Are there any processes to handle the patches to take care of the various vulnerabilities where the critical security updates are managed centrally?	8.8, 8.19	6
Laptop Security	SQ16.	Does the antivirus software installed in your organization's devices have the malware protection capability?	8.34, 8.16, 8.7, 5.7, 5.14, 5.23, 6.7, 6.8	7
	SQ17.	Are the endpoints or laptops provided by your organization encrypted?	8.1	11, 4
	SQ19.	Do your organization provide any remote working tool for secure remote access?	6.7	11
Business continuity	SQ20.	Are there any business continuity plans documented and implemented for your organization?	5.29, 5.30	10

3.3 Survey topics theory

3.3.1 Security Policy (SQ7 and SQ8):

Information security policies play a very important role in protecting our companies sensitive data by providing guidelines and processes for all employees and stakeholders (Computing, 2023). And with evolving threats, the policies must also change to address the new threats and update the compliance regulations (RichardMurphy, 2022).

ISO 27002 outlines the security practices and based on ISO 27001 the ISMS of a company is created. SMEs who are with growth mindset must manage their effectiveness by implementing a holistic approach for policies on standards, privacy and data protection which supports their growth (Levy & Powell, 2004, pp. 37-38).

The figure below shows how the relationship between information systems, technology and management are interrelated to each other. As today's modern digital organizations are critically dependent on information systems which increases complexity, therefore, there should be clear policies on standards, privacy and data protection (Levy & Powell, 2004, pp. 48).

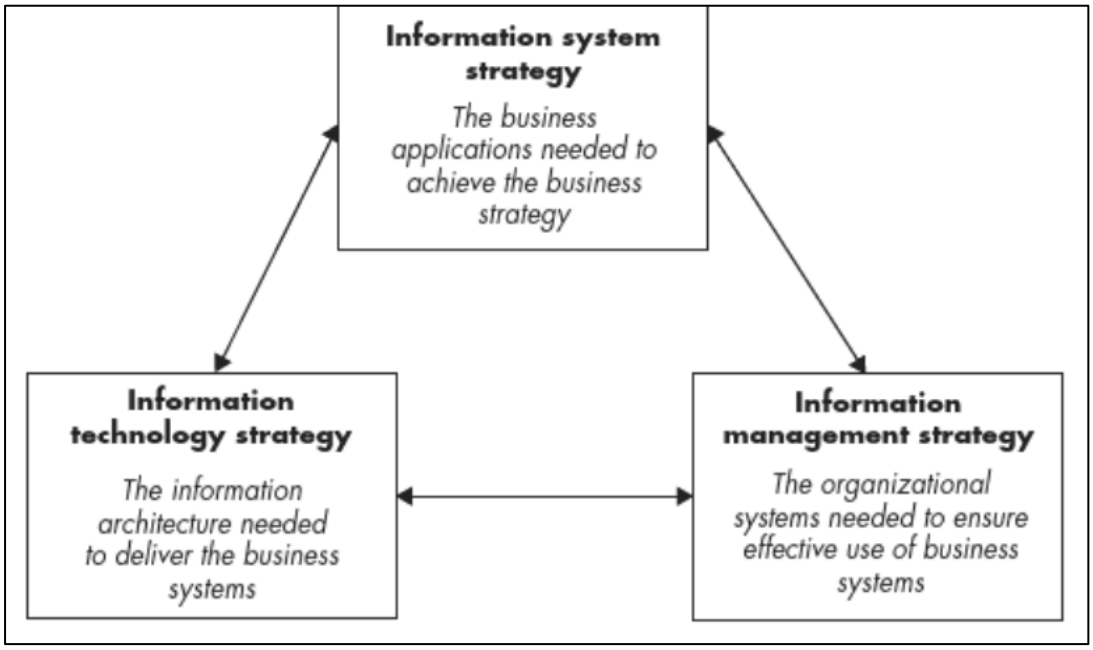


Figure 4: inter-relationship between Information systems, technology and information management (Levy & Powell, 2004, pp. 48).

But as each security risk is unique and apart from the technical related security issues, there are also different and broader risks, so the security policies should also evolve by following different methodological approaches of ISO 27002 that affects data security (Assing & Calé, 2013, p. xi).

Figure below shows the differences between the responsibilities of information security which safeguards all the business data wherever they are, and IT security protects all the technical assets of the organization (Etheridge, 2024).

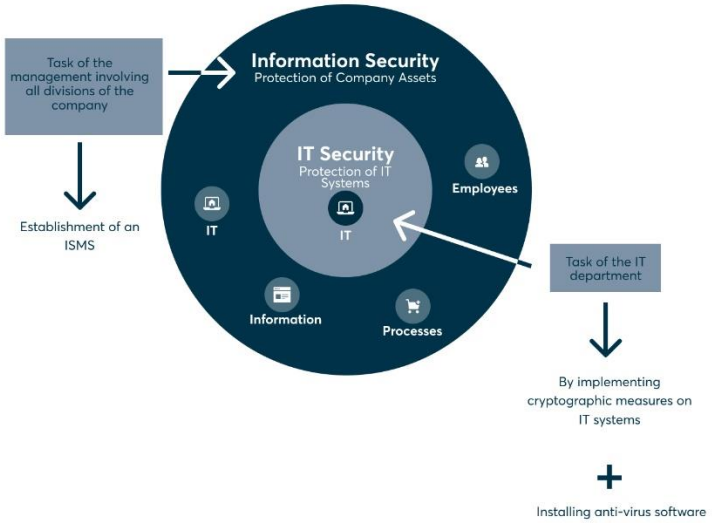


Figure 5: Responsibilities of InfoSec and IT security (Etheridge, 2024)

According to Jibin & Jibin (2024), the main purpose of information security policy is to :

1. Ensure laws and legal are compliant according to customer and industry standards.
2. Provide guidelines for information protection.
3. Manage security practices and clarify employee responsibilities.

The best practices for implementing information security policies, according to BraunWeiss (2024) are:

1. Risk assessment.
2. Policy development.
3. Employee training.
4. Continuous monitoring.
5. Regular review.

According to Jibin & Jibin (2024a), the leadership management team plays a pivotal role in implementing information security policies by ensuring:

1. Policy alignment.
2. Clear information security objectives.

3. Reviewing the policy and implementing it effectively.
4. Commitment to legal requirements.
5. Communicating the purpose of the information security policy.

There are different information security policies which includes access control, password management, incident management, vulnerability management, supplier management, device policies etc. (Rüdell, 2025).

But due to lack of resources that can manage the various complex cybersecurity challenges, SMEs can take the help of security consultancy firms. Taking the help of a consultant can be cost effective but can evaluate the different areas and provide guidance and support by implementing proper ISMS and its policies by considering the company's own business needs (Chakkalakal, 2024).

Therefore, Infosec policy implementation helps to bring in more business by strengthening customers trust and supports long-term success in businesses (BraunWeiss, 2024).

3.3.2 Accessibility of documents (SQ9 and SQ10):

Information security awareness training educates its employees starting from the executive level about the different security related issues and provides best practices to identify the various cybersecurity threats in the modern technology world (Infosec Institute, 2023). It helps to identify and reduce different associated risks that addresses both the human and technical aspects (Keepnet Labs, 2025).
Training materials should be tailor-made, simple and easily understandable for all the employees, so they should contain relevant and updated materials for which help from security consultancy firms can be taken as creating the materials by self can be time-consuming (Infosec Institute, 2023).
It is not a one-time activity, but a continuous cycle to help employees handle confidential informations responsibly and it can include relevant real-life incidents related to the company’s industry type (Keepnet Labs, 2025). It helps in fostering our security culture and encourages employees to identify, be vigilant and report any kind of suspicious activities (Keepnet Labs,

2025). The figure below is used to explain the lifecycle of the security policies and it's related security awareness trainings by using the PDCA cycle.

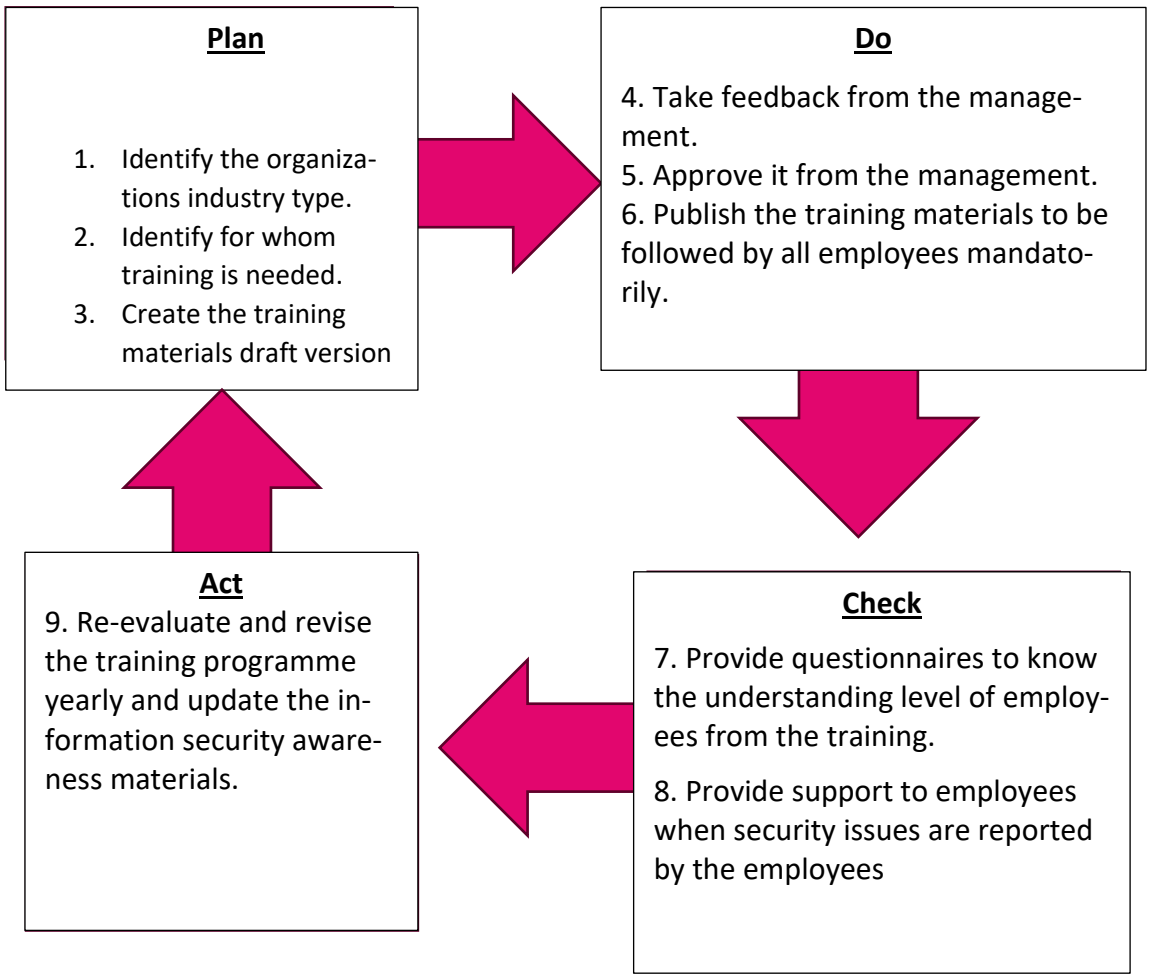


Figure 6: Lifecycle of security policies and information security awareness training materials

It educates and influences the employees attitude towards information security incidents (Khando et al., 2021). Therefore, the infosec trainings should be provided in the form of webinars and recorded videos and the questionnaires from the materials and the policies should be also asked (Stabelin, 2025).

The training materials and the company's security policies should be familiarized to the people on the day they are onboarded and it should be made available in the company's intranet so that the relevant policies and training materials are easily available to all employees when needed (Risk Ledger, 2022).

For long-term business success and growth, with the support of leaderships initiative and employees engagement, security compliance can be achieved when the training modules and policies that covers all the relevant and effective details are made available on the company's intranet or in some easily accessible internal portal (Miller, 2024).

3.3.3 Data Privacy(SQ11 and SQ12):

EU's General Data Protection Regulation (GDPR) introduced in May 2018, which was built on DIR 95 is applied all over EU or EEA, but the way of implementation may be different country wise according to the national law (Brodin, 2019).

Although achieving data protection is a global challenge and with time it's evolving as international markets from different continents have to protect EU residence data while handling data securely (Aristotle, 2025).

GDPR compliance can be achieved by auditing what personal data is collected, why the personal data is needed, where it is stored, and who can access it (Brodin, 2019).

Proper training should be provided about personal data handling for the employees in order to protect privacy rights and prevent fines and legal issues (Trust in Digital Life, 2018).

GDPR has raised awareness about data protection globally and is evolving from national laws to a worldwide approach (Aristotle, 2025).

Therefore, SMEs must implement data protection principles in all business processes and systems by ensuring privacy is always enabled or implemented as a default setting (Trust in Digital Life, 2018).

GDPR regulations have brought in major changes in all organizations. But for SME's, they lack resources and knowledge (Brodin, 2019). With time after COVID-19 and modern warfare, GDPR has improved the data privacy rules in the EU and is evolving globally, although improvements are needed in enforcements, compliance cost and user consents (Kavya, 2025).

Being GDPR compliant is essential for all businesses and by adhering to it SME's can build trust and secure their business and navigate data regulations which can make their businesses grow by bringing in more customers (Limited, 2023). According to GDPR, personal data that directly or indirectly identifies a person must be collected

and processed lawfully, transparently and for specific purposes only. Therefore, companies that collect such kind of data must ensure secure access, clear consult and security breach reporting within 72 hours (Usercentrics, 2024).

In today's competitive, data-driven technological world, GDPR applies to all companies within EU and non-EU companies who are providing services to EU customers as well (Usercentrics, 2024). And with the rapid growth in trade landscape and strict compliance, SME's must adopt strict data protection practices, regular employee training through gamification, encryption, regular updates, and strong governance (Samira et al., 2024).

GDPR mandates business in or with EU companies should implement end-to-end encryption for cloud storage by ensuring operational security. Through policies and training (Pansy, 2024). GDPR regulations have brought in major changes in all organizations, but for SMEs it has brought in various challenges as it uses too many systems (Brodin, 2019):

a. Too complex and heavy.
b. Very costly.
c. On availability of Data Protection Officer, DPO, who is knowledgeable about the GDPR regulations.
d. Lack of awareness of cross-border data transfers.
e. Lack of proper processes for any incident response.

SMEs should always opt for storing data in cloud instead of storing data on-site as using cloud enhances security, reduces cost and provides inbuilt maintenance by the software providers and help and support operation during any disasters (Thakral, 2022). There are many cloud solutions available in the market, but Google and Microsoft are the most reliable ones as it helps in secure collaboration, monitoring and sharing data securely (Schwebius, 2024b).

Benefits of using cloud services are (Schwebius, 2024b):

f. Reduce expenses in maintenance and cost effective.
g. Data access anywhere, anytime, on any secure device.
h. Encourage collaboration.
i. Accessing confidential data securely by implementing encryption. SSO and enabling authentication.
j. Role based access.

k. Enables automatic integrations with third party approved applications.
l. In built AI.
m. Ability to choose data storage region.
n. Automated reporting and monitoring.
o. Secured data backup and restoration.
p. 24/7 customer support

3.3.4 Software usage (SQ13, SQ14, SQ15 and SQ18):

SME's often faces damage due to common cyber-attacks like phishing ransomware and inside that threats which leads to data breaches reputation loss financial loss (Papathanasiou et al., 2025). In today's competitive technological applications cloud technology solutions are easy to go softwares as cloud computing supports software as a service SaaS models which help in easy management of the accesses and permissions by the items and the vendor can manage their software upgrades for the cloud version (Thakral, 2022b). Compliance with GDPR regulations are very important as it involves legal and financial issues and customers trust is also at risk (Papathanasiou et al., 2025).

Cloud-based services has the pay-as-you go model and are reliable, stable and scalable which makes SMEs avoid advance payments, adapt to easy growth, helps in managing the IT part efficiently and cost effectively, helps in business growth and maintain the cloud operations during disasters (Thakral, 2022b).

Software inventory of all the existing and new systems should be listed somewhere so that it is accessible anytime by anyone responsible when needed (Schell, 2015).

SaaS software applications which are accessible online, the access provider should be responsible only to take care of the services and infrastructure and data availability as they have access to the data center. But the SaaS customer, especially the IT team is responsible for providing access to the users. check the policy and compliance security settings, marketplace apps integration, data backup for data recovery when needed due to accidental deletion (Parlikar, 2022).

When any software is evaluated, CISO and the IT managers should check and review the compliance and security setup, data residency according to the GDPR, end-to-end data encryption, SSO or MFA should be setup to prevent unauthorized access, tracking of user activities via audit logs (Josys, n.d).

When a new software is considered to be taken into use in the organization, first it's checked for what purpose it's needed, budget approval, evaluation of the security policies of the app and then the final proposal with the vendor is discussed and after the contract is signed, the new system is setup and then providing relevant users access to the tool (Schell, 2015). Different steps involved when using a new software in a company is shown below:

Table 4: New software implementation process

Proposal team	- Analyse the business requirement for the tool	
	- Price check and it's hidden cost	
	- Security	- Data storage
		- Privacy policy
		- Type of personal data collected
		- Support policy
Approval process	- Financing discussion	- Any offers
		- Pay-as-you-go
	- Approved by CISO and IT team	
	- Signing contract	
Implementation process	- Setup the new system by IT	
	- Decide the type of accesses users could be provided to reduce license cost	
	- Testing the new system with a pilot team	
	- Training for IT, how to maintain the new system	
	- Future roadmap and improvement of the software by the vendor	

When planning to buy a new software, ask the vendor for live demos about all the features and if there's any hidden cost in accessing those new features, check for reviews and take references from colleagues, customers and online user community, different type of licensing models, end users training materials and the team or department who will be using the software primarily (Be the business, n.d).

According to Lanchec (2024), after a new software is purchased, IT Manager and the admins should follow the best practices for proper access control like.

i. Enforcing multi factor authentication (MFA) if available from the admin settings, otherwise if only user is able to enable the MFA or two factor authentication then ask the user to enable it, as it adds extra security layer to prevent unauthorized access when users log in password is stolen. In today's digital world, it's a crucial security measure to enable multifactor authentication.
ii. Enforcing strong password policy according to the company's ISMS password policy.
iii. Implementing Role based Access Control (RBAC) to give access to the licenses according to the roles to protect the sensitive data and prevent unauthorized access.
iv. Regularly review and update the access permissions of the users so that proper accesses and licenses are provided based on their task and remove unnecessary permissions as this might also reduce the cost when some softwares are very costly, by following Principle of Least Privilege (PoLP).

All the list of software and hardware assets should be documented in a centralized location which can be accessed anytime when needed and should always be kept up to date which contains details like cost, account details, who are the primary admins and the same inventory can be used to record the licenses and devices assigned to the employees and its own contractors so that accesses can be revoked during off boarding process (Adams In-Security, 2024).

Softwares which are used for work purposes in work laptop should be taken care of to protect against the various cyber threats that exploits the outdated softwares and therefore patch management is important for SMEs to protect the company's sensitive data and prevent data breaches by safeguarding the assets, to maintain the brand reputation and it's future business prospects (Team, 2023). With the growth in technology, digital platforms and interconnected businesses, SMEs should start identifying the various cyber risk early to reduce the data breaches, ransomware attacks and other threats that exposes sensitive data (Papathanasiou et al., 2025).

Patch management is a type of preventive control method to lower the vulnerability risk (Ohayon, 2024). To fix the bugs and reduce the vulnerabilities of different applications, software developers regularly releases new patches in the form of new features (Firch, 2024). With continuous patch management process, immediate identification and prioritization of vulnerabilities are done, which reduces, supports compliance and improves the cybersecurity posture (Firch, 2024a).

Operating systems and all the desktop applications should be kept up-to-date to protect against vulnerabilities (Papathanasiou et al., 2025). Matches should only be applied or downloaded from trustworthy and reliable vendors after it's identified and it should be scheduled in a fixed time slot (eBanking but secure, 2021). A proper patch management tool should be chosen that meets the needs and is also easy for administrators to use. Therefore, there should be patch management policy implemented for applying patches in order to address the changes in cyber threats and technology and to foster a security culture among all the employees (Team, 2023). Licensed software should be used as it's created by real developers as it protects against the new threats as legitimate softwares receives regular updates to fix the vulnerabilities and reduces the risk of outdated and open source softwares (Papathanasiou et al., 2025).

IT team should also subscribe to some sources in order to keep information or updated about the available vulnerabilities and patches so that critical vulnerabilities are addressed and such reliable sources are like CERT websites, software’s official announcement site and other cybersecurity websites (Ian, 2025).

Nowadays, automated system update management tool can also be used in order to prioritize the updates regularly (Papathanasiou et al., 2025). Continuous patch management can be achieved by utilizing through automated updates as it increases the efficiency, consistency, rapid deployment and reduced downtime (Firch, 2024c). But with limited budget and high cost, implementing any kind of SIEM tool for real time monitoring might be difficult by SMEs but it should be planned in the future road map when the company grows (Lanchec, 2024). Otherwise, manually the team have to check the vendor websites and then ask the users to perform the necessary updates which might delay the software to get updated as there isn't

any automated tool to identify, monitor and push the patches remotely or automatically (Ian, 2025).

The most vulnerable softwares are the end-of-life (EOL) softwares that are no longer supported or updated by the vendors and these softwares possess high risk due to lack of updates and are more attractive to data breaches (Timalsina, 2025). The EOL softwares contains serious risk and exposes the endpoint to security threats (Chainguard, 2024). The risk of using EOL softwares are (McDowell, 2019):

i. File compatibility problems.
ii. Software will crash and develop bugs.
iii. Makes the device more vulnerable due to the presence of the EOL software, which can be exploited by the hackers.
iv. There might be regulatory and legal issues.

Therefore, the EOL softwares should be uninstalled and upgraded timely in order to protect data and keep the system free from security threats. Nowadays most of the software's while installation asks the user to receive automatic updates enabling the functionality to keep the software up-to-date (McDowell, 2019).

3.3.5 Laptop security (SQ16, SQ17 and SQ19):

SME's are at higher risk for malware and other cyber threats, so it should invest in antivirus (AV) solutions which provides real time defense against various viruses and malwares, provide automatic updates of the installed softwares, remote scanning functionalities on both the Mac and Windows systems and should also have the EDR functionality which gives real time alerts via mail to the IT team when any kind of malware related issue is detected (Spector IT, 2024).

Although a good AV gives a good protection, but it should also be made sure that it doesn't slow down the computers, which will then make resources to disable the functionality (Bhoot, 2023)

EDR functionality in an AV is an endpoint security system that detects and alerts any kind of anomalies and quarantine or isolates the malicious files (Soleman & Soewito, 2024).

In the market, both paid and open-source antivirus solutions are available, but when considering the business growth alongside various requirements, it is always advisable to opt for the paid version as the complexity of the securing endpoints is increasing and the digital threat landscape has evolved rapidly, and is very concerning (Shu, 2023). Open-source software relies solely on community support and does not provide any official assistance in the event of any software issues.

SME's should prioritize affordable, reputable, real-time threat monitoring, advanced analytics and robust antimalware solutions in order to protect businesses against and remove malicious software (Papathanasiou et al., 2025)

Hackers can create new malware signature by changing the code and modifying any existing malware, but today's EDR functionalities has built in AI feature which detects the threats based on the different suspicious activities rather than the known signatures which identifies any kind of malicious activities and it immediately isolates by moving any infected files to quarantine, providing a robust protection (Tovey, 2020).

AV's for the endpoints should be centrally managed without any user intervention, making it easier for IT team to manage the updates and configurations remotely and enforcing auto updates as scheduled (Edwards, 2003)

Automation can manage all the approved and disapproved malwares and prioritize its procedures and as a result improves threat detection and responsibilities, but these AI driven EDR tools must be configured according to the GDPR and country specific laws so that any company using this kind of AV tool should look into the privacy related concerns (Kaur et al., 2024). But it shouldn’t be any issue as different profiles can be configured for different restrictive data protection laws.

Business data moves through various platforms, therefore, to prevent data breach and to maintain customers trust, encryption of data is very important as it protects data both at rest and in transit (Etheridge, 2024). As work-related data are mostly in laptops so device encryption is very crucial and the encryption should be properly configured to protect the confidential data from unauthorized access and this can be achieved by implementing a proper mobile device management (MDM) (Trio Team, 2025).

Without encryption, any important information can be easily stolen by cybercriminals and as a result when the device is lost it can lead to heavy fines and legal issues when it contains any kind of customer-related data according to GDPR, which can lead to loss in company’s reputation and loss of trust by customer (Etheridge, 2024).

As the company grows and there is an increasing amount of customer data, implementation of MDM should be already planned as it helps in (Trio Team, 2025):

i. Remote monitoring.
ii. Remote patching.
iii. Remotely applying the security policies.
iv. Enforcement of. Password complexity enforcement.
v. Wiping the device remotely when it's lost.
vi. Facilitating secure softwares installation from the managed apps list.
vii. Managing firewall settings.

In case of laptops, SMEs can use the built-in encryption feature of the laptops to keep the data secure where it encrypts the full disk. (Etheridge, 2024)

i. In Windows: BitLocker key should be turned on and the key can be saved in Personal Walk Drive folder or synced to the work Microsoft account.
ii. In Mac: File Vault key should be enabled and the recovery key can be saved in personal Work Drive folder or in personal iCloud account if not specified.
iii. In Linux: Encryption of the disk happens during the OS installation.
iv. In Android phones: Encryption can be enabled from the device settings.
v. In iPhones: Encryption can be also enabled from device settings and by default data is encrypted there when a passcode is set.

When working remotely, employees should be very vigilant, as it has different risks than working in an office (Cyber.gov.au, 2024). There should be Secured Remote Teleworking Policy defined which make it easier for employees to follow when working remotely (Williams, 2018). Laptops or any kind of work-related devices should not be kept unattended, should be always kept locked and the work device should not be shared with other members of the house or shouldn’t be used for personal purpose in order to prevent data loss (Cyber.gov.au, 2024). When working remotely or traveling, VPN should be used to protect the identity on public networks, so employers should always provide a VPN in order to access the work files and applications through a secure tunnel over the Internet (Rivera, 2024). Public Wi-Fi are very unsafe and therefore sensitive files should be avoided while accessing work related stuffs in public and instead home Wi-Fi or personal hotspots should be used in order to access work

related stuffs (Cyber.gov.au, 2024). While remote working, information leaks, misuse and unauthorized access should always be prevented (European DIGITAL SME Alliance, 2018). Therefore, use of any work related paper documents should be restricted and if it's needed then it should be stored in a secure place and should be disposed securely using shredder or by secure disposal (Williams, 2018).

3.3.6 Business Continuity (SQ20):

Business Continuity Plan helps the SMEs to handle the economic shocks, manage crises, promotes long term stability and also helps business growth and efficiency in the long term (Anjorin et al., 2024).

Many SME businesses without a business continuity recovery plan may never reopen or recover and looses customer's trust (Stasiak, 2022). Figure below are few examples for which BCP should be implemented.

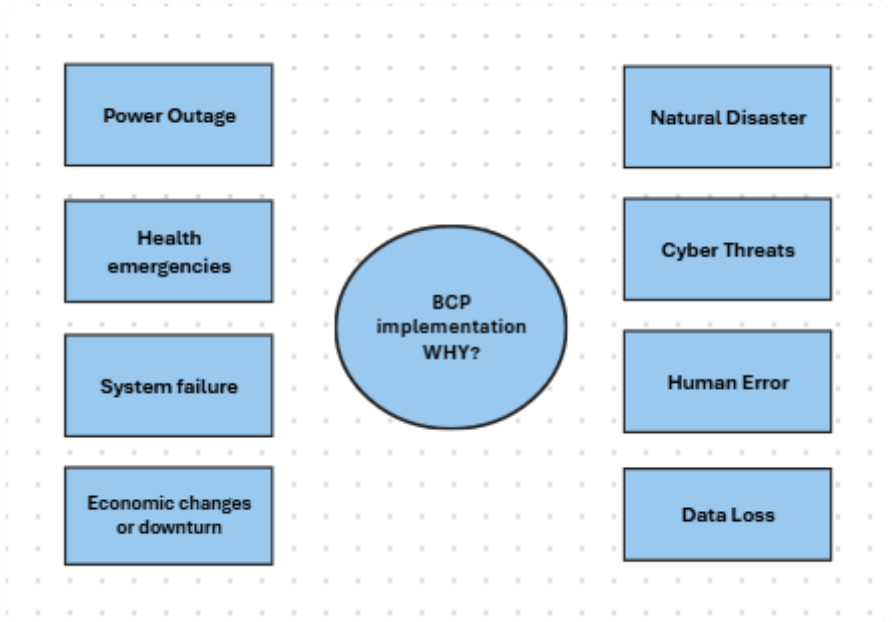


Figure 7: Reasons why BCP should be implemented (Stasiak, 2022)

During and after any kind of disasters like natural disasters, cyber-attacks etc. the business continuity helps the organizations to maintain the essential functions and operations in order

to minimize the downtime and to quickly recover and return to normal operations with minimal interruptions (Gillis, 2024).

In order to recover from any disruptions and keeping the business running by keeping it stable and resilient, SME should ensure (Nepfumbada, 2017):

i. Secure working locations.
ii. Identify the redundant and critical IT systems.
iii. Keep regular data backups if not available from the vendor.
iv. Maintain data protection.
v. Identify critical business processes.
vi. Identify alternate secondary systems to use in case of disaster and failure of the primary IT system to keep the minimum level of acceptable IT systems in use during disruptions to keep the business running.

BCP processes as mentioned in ENISA (2010) are:

i. Identify or establish the BCP team with their contact details, sample below

BCP Team			
Department 1		**Department 1**	
Employee 1	Employee 2	Employee 1	Employee 2
Name	Name	Name	Name
Department	Department	Department	Department
Title	Title	Title	Title
Phone	Phone	Phone	Phone
Email ID	Email ID	Email ID	Email ID

Figure 8: BCP team (ENISA, 2010)

ii. Alternative business processes or systems when there's any disruptions

Assets/Softwares				Damage/Disruptions			Alternative business action		
Name	Description for what purpose it's used	Support contact details	Criticality	Details of the disruption	Time and date of the disruption	disruption and downtime info from the vendor	Name	how it can replace the existing asset temporarily	

Figure 9: Alternative business process during disruption (ENISA, 2010)

iii. Identify the list of suppliers with their contact details.
iv. Test it out with the employees
v. Review the process annually to ensure everything is up-to-date.

Benefits of business continuity plan are (Arbelos, 2025):

i. Provides risk assessment of the IT systems and processes.
ii. Provides data backup solutions for quick recovery of data lost from IT disruptions.
iii. Improves IT security by accessing advanced cybersecurity tools to ensure resilience against data breaches.
iv. Implements scalable IT infrastructure to keep the business grow.
v. Reduces disruptions.

4 Survey Analysis

4.1 To whom the survey was sent

The survey was sent via e-mail and web link to 10 companies and only 4 have responded. Before sending mails to other small companies, they were contacted first but answering to the survey was denied due to non-availability of NDA. It's always advisable to get permission from a member of the management team to answer the survey due to privacy reasons and to maintain confidentiality and integrity of internal processes.

4.2 Survey topics and questions

In the survey there were total 21 questions out of which:

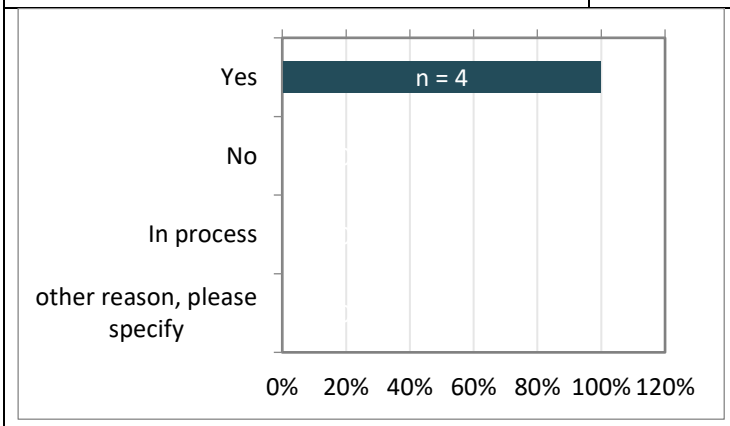
i. questions 1 – 5 were about the introduction of the respondents
ii. question 6 was about the total number of employees in the company
iii. questions 7 - 20 were related to my thesis topics
iv. question 21 asked about the feedback.

4.3 Survey results

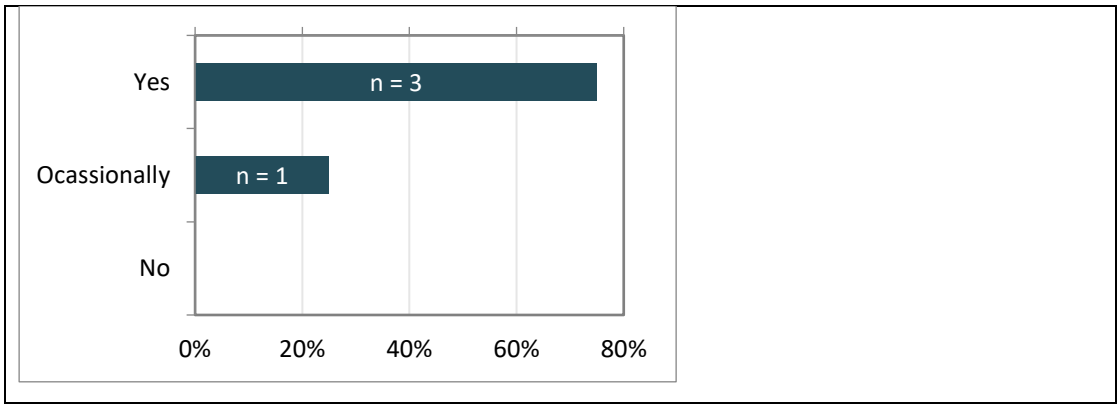
4.3.1 Security Policy (SQ7 and SQ8)

Table 5: Survey results for survey questions 7 and 8

SQ7: Does your organization have its own documents and policies so that the employees can comply with the information security standards in order to prevent data breaches of sensitive and confidential information?	**Answers**	**N =Count**	**Percentage**
	Yes	4	100,0%
	No		,0%
	In process		,0%
	other reason, please specify		,0%



SQ8: Are the security policies at your organization reviewed and updated at regular intervals?	**Answers**	**N =Count**	**Percentage**
	Yes	3	75,0%
	Ocassionally	1	25,0%
	No		,0%



In the survey all the 4 respondents have agreed that they have their own information security policies set up within the company for the employees and which is reviewed at regular interval.

Security policies should always be available irrespective of any size of the company and this includes even the micro enterprises companies. It can start with a very simple policy, doesn't need to be very complex, but a bare minimum in order to safeguard the business and progress in business growth.

The security policies should be taken care of by someone in the company who is technically skilled and is familiar with the information security policies, it's rules and laws and should be approved by the management team. The policies should be simple and easily understandable by employees of all categories. Later, when the company grows and the number of employees and customers increases, the information security controls can be implemented in a detailed way, and if a designated CISO is not available, then it can be outsourced who can plan and implement security policies for different topics like asset management, password management, data handling, access control, data privacy and confidentiality, physical security, supplier policy, etc.

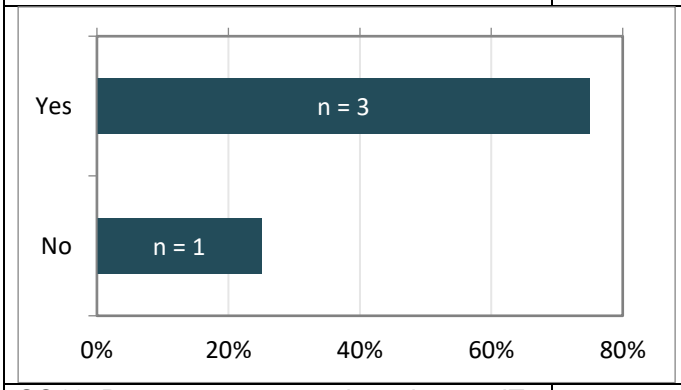
Security policies should always be kept up to date whenever there is any major change and should always be reviewed yearly. Starting from bare minimum, information security policy will not only protect the business, but will also help the employees in the company to respect and comply with the rules and regulations set by the company and will have a strong foundation of confidentiality, availability and integrity of business processes.

4.3.2 Accessibility of documents (SQ9 and SQ10):

Table 6: Survey results for survey questions 9 and 10

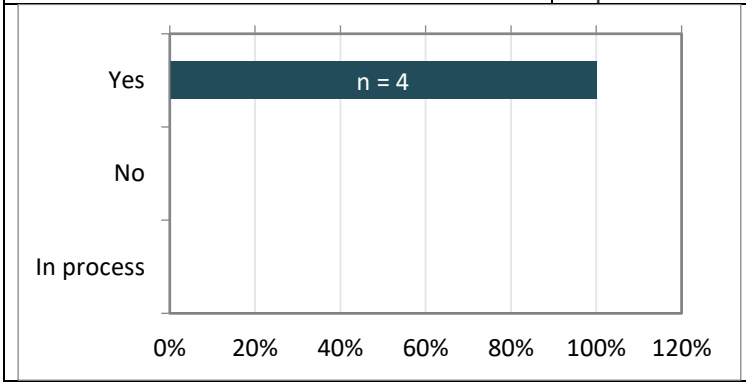
SQ9: Are the documented security policies at your organization easily accessible and understandable by the employees?

Answers	N =Count	Percentage
Yes	3	75,0%
No	1	25,0%



SQ10: Does your company have its own IT security training materials available for the employees to ensure that they know how to handle the sensitive information?

Answers	N =Count	Percentage
Yes	4	100,0%
No		,0%
In process		,0%



In the survey, 3 respondents have agreed that their company's security policies and training materials are easily accessible by their employees. And 1 respondent have only agreed that the IT security training materials are available for employees, but the security policies aren't easily accessible by the employees. But hopefully access is provided when requested.

Employees are the real drivers for the growth of a business and as they work closely with clients, so they are more susceptible to get affected by the security incidents. In today's digital world if an employee is not aware of the digital threats then they are at a major risk or prone to cause any kind of data breaches from minor to high incidents caused by the human error, therefore, all the employees irrespective of any industry should familiarize themselves of the information security training materials which can be in the form of webinar as well. Employees should be familiarized with how to prevent data breaches and cyber risk by keeping themselves updated by imparting a security minded culture to protect the organization from the new cyber threats by being vigilant. Preparing the training materials can be very time-consuming and it needs an expert who is familiar of the information security world, so it can be also outsourced to a security consultant and who also knows how to keep their employees motivated by conducting and familiarizing the cyber breaches in the form of quizzes, gamification, showing real life examples. The common topics which the training materials should cover are:

i. How to protect and manage confidential data.
ii. Not to open any kind of suspicious links or attachments.
iii. Maintain strong password policy.
iv. Use only company provided softwares and devices for work purposes.
v. How to use internet securely.
vi. Where to report when any kind of security incidents or breaches happens.

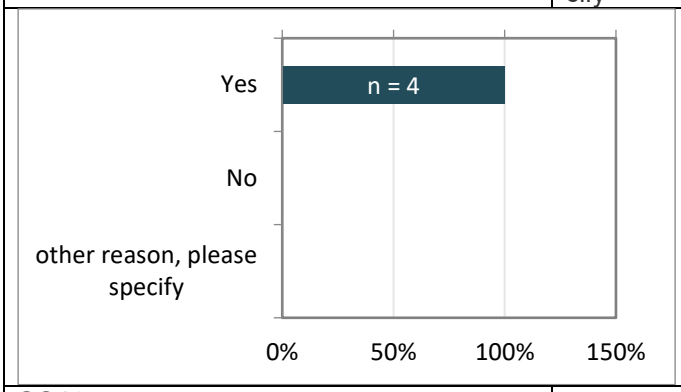
Management plays a pivotal role in prioritizing and mandating the importance of information security training awareness and as a result it will develop a security conscious culture leading to a cyber resilient and secure organization.

Also, these security policies and the training materials should always be made available and easily accessible digitally and in a centralized place, for example in the companies intranet, so that the same updated information is available when needed to share internally among employees or externally with clients by the employees when needed.

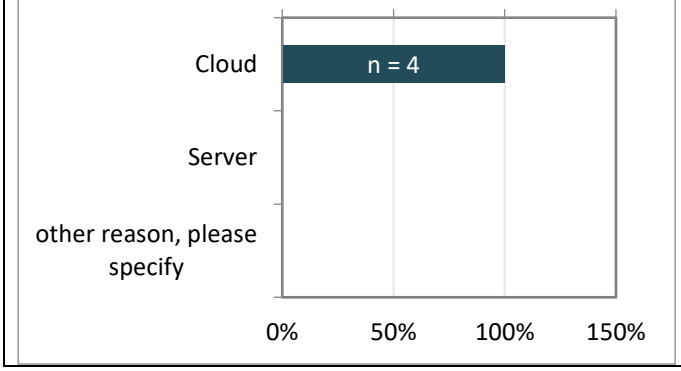
4.3.3 Data Privacy(SQ11 and SQ12):

Table 7: Survey results for survey questions 11 and 12

SQ11: Are the GDPR guidelines at your organization followed while handling your clients/customers data?	Answers	N =Count	Percentage
	Yes	4	100,0%
	No		,0%
	other reason, please specify		,0%



SQ12: Where are your organization's data stored?	Answers	N =Count	Percentage
	Cloud	4	100,0%
	Server		,0%
	other reason, please specify		,0%



All the 4 respondents have ensured that their organizations data are stored in the cloud and it follows the GDPR guidelines for handling the work data.

GDPR is about handling the personal data which focuses on:

i. What kind of, why and how the personal data are collected.
ii. Who will access the personal data.
iii. And how long will the personal data be stored.

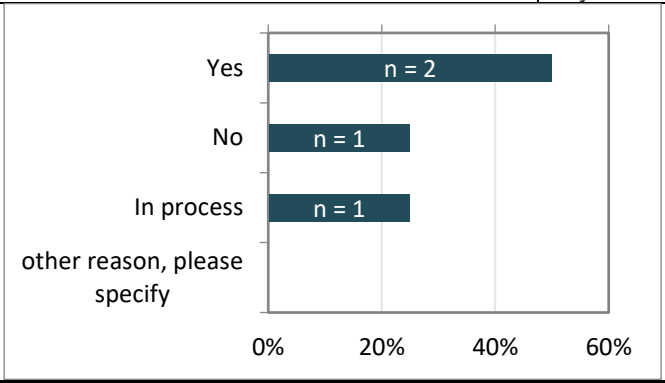
It's an EU law which should be followed by anyone within the EU and any companies doing business within or with EU. So, the mandatory personal data that are collected internally about the employees, only a team of people should have access to it and should be responsible for what kind of personal details will be shared to other teams internally should also be recorded. The main aim of GDPR is to protect people's data from not being misused and are handled by the designated handlers responsibly, securely and transparently.

Moreover, GDPR is also applied to any softwares which are purchased from third party vendors which is used to store any work data. IT should check what kind of personal data the software collects and where the work files are stored, whether it is in EU or outside EU. The clear instruction and training about GDPR can be given only by a DPO or CISO, or else it can be outsourced if the SME doesn't have any data privacy knowledgeable resource. Once the data privacy policy and training materials are ready, it can be shared within the organization for the awareness of the employees and the team who are handling the personal data. Personal data should only be collected based on what is needed and necessary and should be kept confidential and should be recorded where the data is stored, either in cloud or in the company's own server. But for SME's, the only feasible option is storing data in cloud as there is no extra maintenance and setup cost and doesn't have to worry in hiring expert staffs to manage and monitor the servers. As there are many disadvantages in owning a server, so all the SME companies and even the larger enterprises would prefer to use cloud as their data storage. So, making the data available and safeguarding the data is in the cloud provider's hands. But the SMEs are the ones who's responsible for the kind of data they have stored and to whom they have given the different kind of permissions to access the data, and they are also responsible to configure the setup properly so that data compliance can be achieved. If an SME is GDPR compliant then it also helps to gain customers trust and bring in more growth to the business.

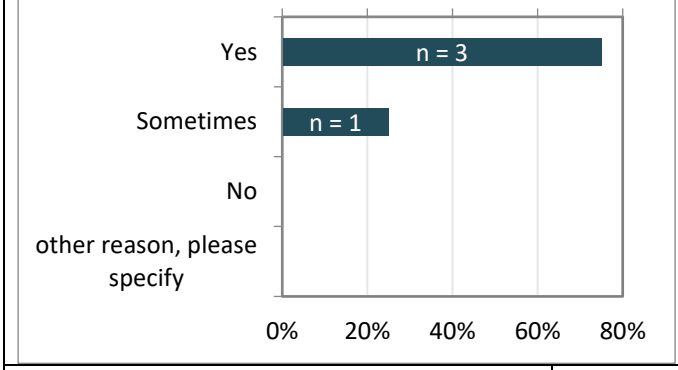
4.3.4 Software usage (SQ13, SQ14, SQ15 and SQ18):

Table 8: Survey results for survey questions 13, 14, 15 and 18

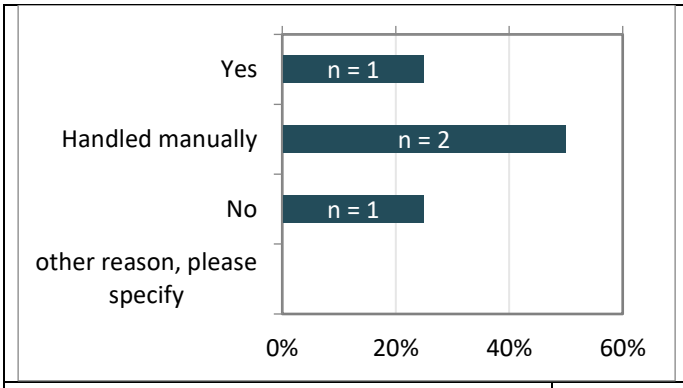
SQ13: Is the multi-factor Authenticator (MFA) enabled for all/part of the softwares used in your organization?	**Answers**	**N =Count**	**Percentage**
	Yes	2	50,0%
	No	1	25,0%
	In process	1	25,0%
	other reason, please specify		,0%



SQ14: When using any software for work purpose is it's security policy reviewed for GDPR purpose like where your organization's data will be stored and what information will it gather?	**Answers**	**N =Count**	**Percentage**
	Yes	3	75,0%
	Sometimes	1	25,0%
	No		,0%
	other reason, please specify		,0%

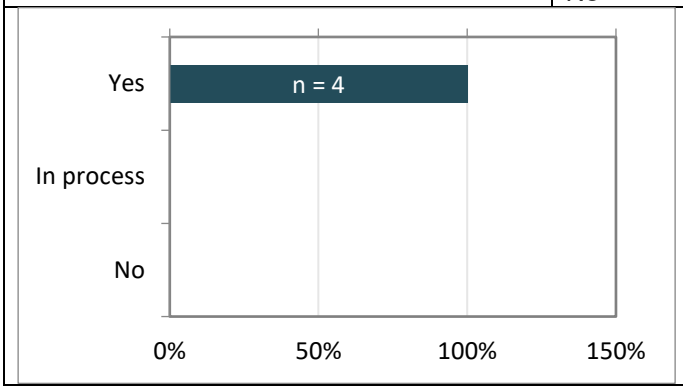


SQ15: Do you organization have any automated way of obtaining the software Inventory if you are working globally?	**Answers**	**N =Count**	**Percentage**
	Yes	1	25,0%
	Handled manually	2	50,0%
	No	1	25,0%
	other reason, please specify		,0%



SQ18: Are there any processes to handle the patches to take care of the various vulnerabilities where the critical security updates are managed centrally?

Answers	N =Count	Percentage
Yes	4	100,0%
In process		,0%
No		,0%



In the previous data privacy topic it was mentioned that GDPR should also be considered when purchasing a software. As mentioned earlier, what kind of personal data the third party applications would collect should always be checked when purchasing any new software and where the data will be stored. Because if the EU data is stored outside of EU region then there will be the GDPR violation. The level of security configuration settings the softwares have should always be checked and if the minimum level of security setup is not available, then the software should not be acquired, even if it provides any new features which will benefit the business. Quite often it is seen that when the company purchase a new software, they look mostly to the business side how the software will bring in more productivity, but the core part that is the security and access configurations are always forgotten and ignored. Therefore, after the software is purchased, all the security configurations should always be checked, changed and tested and reviewed with the IT manager or CISO. And then the software should be made available to be used for business purpose by the employees. With time the setup and

accesses should always be reviewed as sometimes the software receives new admin system upgrades. Access to any files should be restricted and should be given according to the business requirement in order to maintain the confidentiality, integrity and availability of the files in the application.

Another important thing is the kind of authentication setup in the application. As the SMEs are initially able to purchase licenses at a very low quantity, so depending on the caps maybe single user or teams license could be purchased. As the security setup, especially the login authentications are different, so it should be reviewed and ask the users to do the necessary setup if there is user activity involved in setting up of the authentication. But if some kind of authentication can be enforced from the admin side, then that should be also done. MFA enabling is the basic security step which any organizations should implement either by the user themselves or enforced by the applications admin.

If there is a single user license available for a purchased software, then the user should be responsible and take care of the necessary security setup and the details of the software should be shared with IT so that it can be recorded in the software inventory, a secured centralized place which is accessible by anyone in the company when needed for auditing purpose. Gradually when the license requirement grows, if it contributes a lot to the business growth, then the team's license should be purchased for a wider group. In teams license most of the softwares have the capability to enforce MFA which can be enforced. Nowadays by default all the softwares show the password strength of the user while setting it up, so the user should be very careful when setting up the password and should follow the best practices of strong password policies recommended by the company.

Software that are used for work purpose should be always recorded in the software inventory and also record the list of people who have access to the different applications including the owners and admins who have access to the applications admin portal which manages the billing and end users access. If possible, there should be an automated way of managing all the softwares. Maintaining the software inventory also helps to manage the software updates. Those patches which couldn't be updated remotely by the IT team should always be taken care of by the users themselves. IT can share the list of available updates for those softwares in the internal user community discussion. Also, the IT managers should enroll to the NCSC to receive daily newsletters about any kind of zero day vulnerabilities etc. associated with any

kind of work softwares updates which are installed in the user's device. The easiest option will be when there is any automated patch management tool that shows available updates for any softwares available for the end points. Keeping the operating system and the softwares up to date should be the responsibility of both the users and the IT team.

In the survey, 2 respondents have mentioned ‘yes’, 1 respondent has mentioned ‘no’ and 1 respondent as ‘in process’ for enabling the MFA of all the work related softwares. If enabling the MFA for all the work applications is in progress then it is good at least the company is working on it. But if some companies have not at all considered of making the employees aware about the importance of enabling MFA, then they are at risk as MFA is a necessary setting to secure any user accounts.

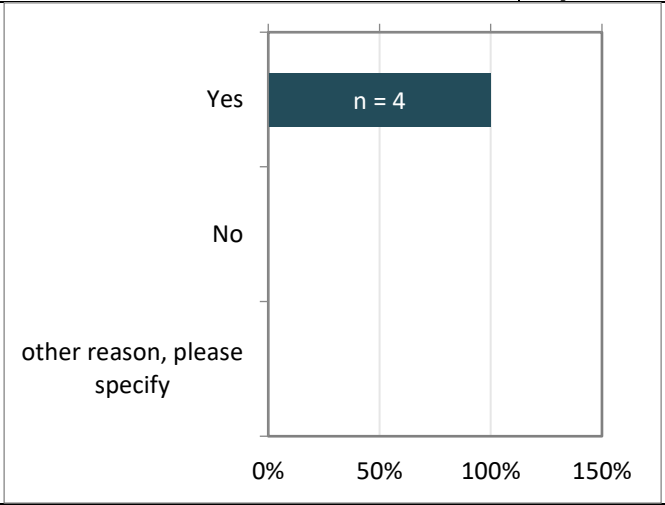
For reviewing the data storage of the work applications, 3 respondents have mentioned that they review it, so it means that they are concerned about the GDPR policy. But 1 respondent have mentioned that they review it sometimes. So maybe they are at least progressing or aware where the application stores data or it maybe they have user based license type for the work applications due to which they are not able to monitor or review it. For maintaining automated software inventory, only 1 respondent have agreed as ‘yes’, and 2 respondents have mentioned that they handle it manually, which is a good process. At least the companies understand the importance of keeping the records somewhere centrally which will help them in future for reference when needed. Whereas 1 respondent have mentioned as ‘no’. So maybe they aren't concerned as of now as taking it manually is time-consuming and maybe they are planning to implement some automated system in near future which will make their task easier and also maybe apart from licensed softwares users are using unlicensed softwares for work.

However, all the 4 respondents have responded that they have a process of taking care of the patches. So either 1 of the company is doing it automatically as they have automated way of obtaining software inventory or all of them are asking the users to do it manually. And hopefully they share the information with the employees whenever there are updates or upgrades available for any installed desktop applications.

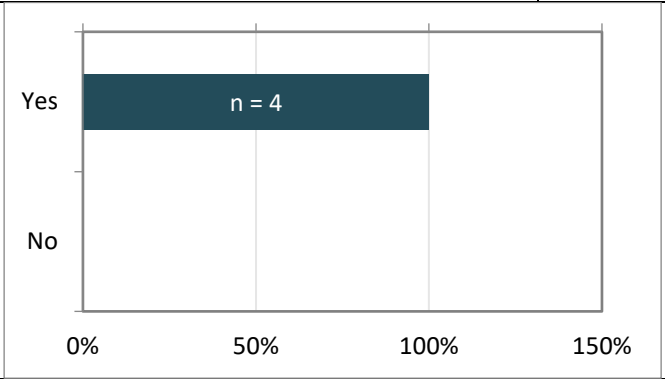
4.3.5 Laptop security (SQ16, SQ17 and SQ19):

Table 9: Survey results for survey questions 16, 17 and 19

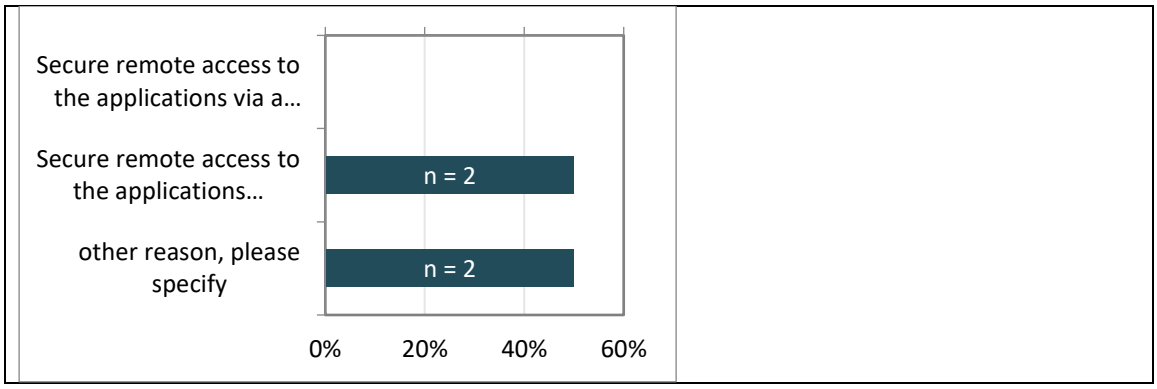
SQ16: Does the antivirus software installed in your organization's devices have the malware protection capability?	**Answers**	**N =Count**	**Percentage**
	Yes	4	100,0%
	No		,0%
	other reason, please specify		,0%



SQ17: Are the endpoints or laptops provided from your organization encrypted?	**Answers**	**N =Count**	**Percentage**
	Yes	4	100,0%
	No		,0%



SQ19: Do your organization provide any remote working tool for secure remote access?	**Answers**	**N =Count**	**Percentage**
	Secure remote access to the applications via a Virtual Machine		,0%
	Secure remote access to the applications using only company's VPN	2	50,0%
	other reason, please specify	2	50,0%



In this survey all the 4 respondents have agreed that they use antivirus (AV) with malware protection capability which is good and hopefully they have activated mail notifications for any alerts that they receive. Any malware files should be quarantined so that user can't recover the harmful file which will prevent the laptop from getting infected by the malware and if the file is needed then after proper investigation by the security team it can be made available to the user. SME's can get support from the antivirus's technical support team. Therefore, it's very important to know if the vendor will be able to provide technical support when needed, and if needed, service can also be paid. It's always recommended to go for an AV solution which has the market name as the protection capability is extensive and sometimes the license cost and the consultant prices are also affordable. AV's should have the basic features like continuous real time monitoring of any harmful files, provide auto scanning and auto update of the software, provides list of outdated or unpatched operating systems or softwares. Same AV software should also be compatible with Windows, Mac and Linux. The AV should also have the firewall protection which can contain the vendors default or company's own custom configuration. The firewall custom configuration might be difficult by the SME as collecting all the relevant data might be so it's better to take the AV's own default configuration as the vendor will always update their own AV's security settings based on their latest security threat report.

Encryption of the devices is one of the most important security features that every company should enforce. In the survey, all 4 respondents have agreed that encryption is enabled for their employees work devices. Enabling the encryption also means that recovery key of the device should be also saved somewhere safe so that it can be provided when needed, for example when laptop's password is forgotten. In Windows, the inbuilt BitLocker key should be

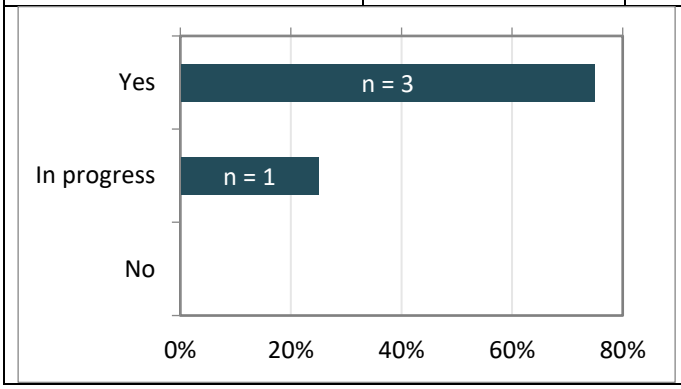
enabled, and the key can be saved in the Azure portal which the IT team who has access to the Microsoft Admins portal can provide when needed by the user or the user can save the key in their work drive folder. In Mac, the inbuilt File Vault key should be enabled, and the key can be saved either in the user's work drive folder or if it can be saved in the Mobile Device Management (MDM) portal. Initially implementing MDM can be costlier and needs dedicated IT resource, but it can be implemented when the number of employees and the business grows and the employees work from different countries. But the SME's can start planning to implement the MDM in the initial phase when there are less employees. Identifying a proper MDM needs time, so the IT team can test out some simple, easy to use MDMS by taking some free trial versions and the team can familiarize themselves and study the various security features in the MDM provides and then finally decide on a proper MDM. The benefits of MDM are encryption enforcement, enforcement of strong passwords, remote wiping when the device gets lost, providing company approved application portal from where the users can download the approved apps.

For remotely accessing company data from the laptop 2 respondents have agreed that VPN is used as a remote working tool for the employees whereas 2 respondents have selected ‘other reason’. There are various remote access tools in the market and the SMEs should think of providing a secure VPN access to the employees so that users can safely access their data in the laptop through an encrypted network traffic irrespective of any network they are connected to.

4.3.6 Business Continuity (SQ20):

Table 10: Survey results for survey question 20

SQ20: Are there any business continuity plans documented and implemented for your organization?	**Answers**	**N =Count**	**Percentage**
	Yes	3	75,0%
	In progress	1	25,0%
	No		,0%



In the survey 3 respondents have agreed that they have Business Continuity Plan (BCP) implemented in their organization and for 1 respondent it's in progress. The business continuity implementation should be planned slowly when the SME's start to have business and customers growth, so that business operations keep running when there are any kind of business disruptions, software accessing disruptions, natural disasters, power failures, etc. Having a business continuity plan in place makes the employees make proper decisions in emergency situations by following the company's best practices and policies and providing proper support to the customers without disrupting the business.

5 Conclusion and Discussion

This thesis would want to highlight the importance of information security for SMEs by referring to ISO 27002:2022. Due to the increased amount of digital cyber threats during COVID-19 and recent modern cyber warfare, it has become utmost importance for SMEs to develop and improve their ISMS.

Main research question: How implementing information security policies with the help of ISO 27002:2022 would help in strengthening the foundation of information security in an SME company?

Easel 27,002 provides A structured set of controls which guides the SME's to protect its organization's assets from the data breaches and data loss, protecting the confidentiality, integrity and availability of. Data. It provides guidance how to train the employees and making them aware of information security who then contributes to build trust with the customers leading to business growth in a secured and compliant manner (Harvey, 2024).

Creating the information security framework early in today's digital world will protect the company's assets, business and its customers and their trust and will bring in cyber resilience in the company. Information security is a continuous process and if due to any reasons there's lack of resources or finance, it's always worth to outsource some of the activities to the designated consultant experts. Most importantly, investing in employee awareness training, implementing information security policies, investing in good and secure tools to take care of the security of the devices and applications from cyber threat can make an SME company cyber resilient.

Sub research questions: How data prep protection plays a major role in implementing information security. Does having a strong foundation in information security and data privacy lead to growth in business and gain customers trust?

Data protection is essential and is very crucial to implement information security successfully as it protects sensitive data from threats and this can be achieved by providing employee security awareness training as they play a pivotal and crucial role in data handling (Aristotle, 2025).

Businesses that invest in protecting their own assets creates a trustworthy environment which attracts customers, and which brings in good reputation and supports growth (Edwards, 2025).

The SME-ISC guide has highlighted that SMEs should be aware and always be vigilant in maintaining the GDPR compliance, as protection of personal data is a very critical business requirement especially for businesses within and with EU (European DIGITAL SME Alliance, 2018). In order to maintain the confidentiality, integrity and availability of the company's data, employees and customers, SME should follow the 16 security controls recommended by the SME-ISC Guide and the detailed reason of how and why it should be implemented can also be referred to ISO 27002:2022 documentation.

In future, there should be some opportunities if these kinds of surveys could be conducted via the boards who manages and registers the SME companies. But with the NIS2 directive enforced in Finland and in many EU Member States, some SME companies security posture will be improved and the management and IT should work together to strengthen it. Moreover, ENISA provides Cyber Security Maturity Assessment Tool which will help businesses to analyze the level of the security posture and will help to provide a customized plan to improve the security posture according to their business needs (ENISA, 2025). This will help the companies to register to NIS2 and will also help those SMEs who don't have to register to NIS2 due to their company's size and the type of work (ENISA, 2023).

The limitation that I faced during my thesis work was to get the survey answers. As there was no Non-disclosure Agreement (NDA) signed with the companies so it was very difficult to get the survey answers from most of them. So, systematic review method is also used to search for the data and put in my own interpretation.

6 References

Adams In-Security. (2024, June 14). *ISO 27002:2022 – Adams In-Security*. Adams In-Security. https://adamsinsecurity.com/category/assurance/iso-270022022/

Agency for Innovation & Entrepreneurship. (n.d). EU Funding Overview. https://eufunding-overview.be/funding/the-european-union-agency-for-cybersecurity-enisa

Anjorin, K. F., Ijomah, T. I., Toromade, A. S., Akinsulire, A. A., & Eyo-Udo, N. L. (2024). Evaluating business development services' role in enhancing SME resilience to economic shocks. Global Journal of Research in Science and Technology, 2(1), 029–045. https://doi.org/10.58175/gjrst.2024.2.1.0047

Arbelos. (2025, January 15). The Benefits Of Business Continuity Planning With Your IT Provider. https://arbelos.ie/disaster-recovery-business-continuity/the-benefits-of-business-continuity-planning-with-your-it-provider/

Aristotle. (2025, January 29). The development of data protection: from the GDPR to global standards. 2b-advice. https://2b-advice.com/en/2025/01/29/the-development-of-data-protection-from-the-gdpr-to-global-standards/

Assing, D., & Calé, S. (2013). *Mobile access safety: Beyond BYOD*. John Wiley & Sons.

Be the business. (n.d). An SME's guide to choosing software. https://digital.bethebusiness.com/documents/1/Software_guide_full_document.pdf

Bhoot, A. (2023, August 25). Latest Best Antiviruses for Small and Medium Enterprises. *Orion Network Solutions*. https://www.orionnetworks.net/latest-best-antiviruses-for-small-and-medium-enterprises/

Bråthen, R. & Lie, E.K. (2021). Investigating Cybersecurity Awareness in SME Organisations. https://hdl.handle.net/11250/2823146

BraunWeiss. (2024, April 17). *The essential role of information security policies for small businesses*. https://www.linkedin.com/pulse/essential-role-information-security-policies-small-businesses-pvkge/

Brodin, M. (2019). A framework for GDPR compliance for Small- and Medium-Sized Enterprises. European Journal for Security Research, 4(2), 243–264. https://doi.org/10.1007/s41125-019-00042-z

Chainguard. (2024, December 4). *How End-of-Life software accumulates vulnerabilities*. Chainguard Academy. https://edu.chainguard.dev/chainguard/chainguard-images/staying-secure/updating-images/how-eol-software-accumulates-cves/

Chakkalakal, J. (2024, July 2). *Why small businesses must invest in cyber security consulting Services*. Critical Risk Solution. https://www.criticalrisksolution.com/blog/why-small-businesses-must-invest-in-cyber-security-consulting-services

Cheek, P. (2024). Disciplined entrepreneurship startup tactics : 15 tactics to turn your business plan into a business. John Wiley & Sons

*Chegg Writing. (*2021, November 22). Mixed methods. www.chegg.com/writing/guides/research/mixed-methods-research/

Clemente-Almendros, J. A., Popescu-Nicoara, D., & Pastor-Sanz, I. (2024). Digital transformation in SMEs: Understanding its determinants and size heterogeneity. Technology in Society, 102483–102483. https://doi.org/10.1016/j.techsoc.2024.102483

Computing, S. (2023, October 20). *Why you need an information security policy*. Scale Computing. https://www.scalecomputing.com/resources/why-you-need-an-information-security-policy

Critical Risk Solution. (2024, April 30). Why Small Businesses Must Invest in Cyber Security Consulting Services. https://www.criticalrisksolution.com/blog/why-small-businesses-must-invest-in-cyber-security-consulting-services

Cyber.gov.au. (2024). Security tips for
remote working. Australian Signals Directorate. https://www.cyber.gov.au/protect-yourself/staying-secure-online/security-tips-remote-working

DataGuard. (2023, September 4). ISO 27002: All you need to know about the standard. https://www.dataguard.com/blog/iso-27002/#seven

Delev, Z. (2023, December 14). *ISO 27002: A Comprehensive Guide to Information Security Controls*. GDPR Local. https://gdprlocal.com/iso-27002-comprehensive-guide-to-information-security-controls/

Dovetail Editorial Team. (2023, February 20). What is mixed methods research?. https://dovetail.com/research/mixed-methods-research/

Dunham, R. (2020, May 5). *Information Security Policies: Why They Are Important to Your Organization*. Linford & Company LLP. https://linfordco.com/blog/information-security-policies/

eBanking but secure. (2021, March 29). *Patch management in an SME environment. eBas*. https://www.ebas.ch/en/patch-management-in-an-sme-environment/

Edwards, R. A. (2003, September 8). The pros and cons of centrally managed antivirus software. *ZDNET*. https://www.zdnet.com/article/the-pros-and-cons-of-centrally-managed-antivirus-software/

ENISA. (2010, January 12). ENISA report on IT Business Continuity "An Approach for SMEs". https://www.enisa.europa.eu/sites/default/files/publications/BCM_for_SME_Example_BCP-Template.pdf

ENISA. (2023). Diagnose your SME’s Cybersecurity and Scan for Recommendations. https://www.enisa.europa.eu/news/diagnose-your-sme2019s-cybersecurity-and-scan-for-recommendations

ENISA. (2024). SMEs Cybersecurity. https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity

ENISA. (2025). Cybersecurity Maturity Assessment for Small and Medium Enterprises. https://tools.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/

Etheridge, E. (2024). Cyber security measures: Secure your business with digital signatures. Dataguard. https://www.dataguard.com/blog/cyber-security-measures-secure-your-business-with-encryption/

Etheridge, E. (2024, December). What is an Information Security Management System (ISMS)?. Dataguard. https://www.dataguard.com/blog/what-is-information-security-management-system/

European Commission. (2020). User guide to the SME Definition. https://www.european-academy.com/wp-content/uploads/2021/03/SME_definition_user_guide_en.pdf

European Commission. (2024). Annual Report
on European SMEs
2023/2024. https://single-market-economy.ec.europa.eu/smes/sme-strategy-and-sme-friendly-business-conditions/sme-performance-review_en

European DIGITAL SME Alliance. (2018). SME guide for the implementation of ISO/IEC 27001 on Information Security Management. https://sbs-sme.eu/wp-content/uploads/2024/02/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-2.pdf

European Digital SME Alliance. (2022, April). SME Guide on Information Security Controls. https://www.digitalsme.eu/digital/uploads/SME-ISC-Guide.pdf

Fastech Solutions. (2021, March). Fastech Solutions. https://myfastech.com/creating-an-it-security-policy-for-your-small-business/

Fastech Solutions. (2024, April). Fastech Solutions. https://myfastech.com/addressing-common-it-challenges-solutions-for-smbs-small-and-medium-sized-businesses/

Firch, J. (2024, August 19). *Common types of network security vulnerabilities*. PurpleSec. https://purplesec.us/learn/common-network-vulnerabilities/

Firch, J. (2024a, August 18). *The Vulnerability Management Lifecycle (5 steps)*. PurpleSec. https://purplesec.us/learn/vulnerability-management-lifecycle/#elementor-toc__heading-anchor-8

Firch, J. (2024c, November 10). *How to centralize your patch Management*. PurpleSec. https://purplesec.us/learn/centralize-patch-management/

Flanders innovation & entrepreneurship. (n.d.). The European SME definition. https://www.vlaio.be/en/subsidies/ecology-premium-plus/which-enterprises-and-ecological-investments-are-eligible-ecology-premium-plus/european-sme

Flyktman, J. (2016). Implementing Information Security Management System as a part of business processes : Where to gain competitive advantage for ISMS? https://urn.fi/URN:NBN:fi:amk-2016060311816

Gillis, A. S. (2024, April 16). business continuity. Search Disaster Recovery. https://www.techtarget.com/searchdisasterrecovery/definition/business-continuity

Harvard Catalyst. (2022). *Mixed Methods Research*. https://catalyst.harvard.edu/community-engagement/mmr/

Haucap, J., Fritz, D., & Thorwarth, S. (2022). THE ECONOMIC IMPACT OF CLOUD COMPUTING IN EUROPE A research report commissioned by the European Cloud Alliance. https://www.europeancloudalliance.com/wp-content/uploads/2022/11/Cloud-Computing-in-Europe-fin.pdf

Ian. (2025, March 14). The Ultimate guide to patch management for small businesses. Steadfast Solutions. https://www.steadfastsolutions.com.au/insights/the-ultimate-guide-to-patch-management-for-small-businesses/

Infosec Institute. (2023, July). Security awareness: history, types & best practices. https://www.infosecinstitute.com/resources/security-awareness/security-awareness-definition-history-types/

Jibin, A., & Jibin, A. (2024, November 29). *Why SMEs need an Information Security Policy: Insights for Leaders*. Security Quotient. https://securityquotient.io/why-smes-need-an-information-security-policy-insights-for-leaders/

Jibin, A., & Jibin, A. (2024a, November 29). *How leadership influences the implementation of information security policies in SMEs?* Security Quotient. https://securityquotient.io/how-leadership-influences-the-implementation-of-information-security-policies-in-smes/

Josys. (n.d). Evaluating SaaS Applications: A Checklist for IT Managers. https://www.josys.com/article/article-saas-management-evaluating-saas-applications-a-checklist-for-it-managers#1-security-and-compliance

Karaoulanis, A. (2020). Small business management : A road map for survival during crisis. Business Expert Press.

Kaur, H., Sl, D. S., Paul, T., Thakur, R. K., Reddy, K. V. K., Mahato, J., & Naveen, K. (2024, August 9). Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive review. *E3S Web of Conferences*, *556*, 01006. https://doi.org/10.1051/e3sconf/202455601006

Kavya. (2025, February 24). The GDPR impact: Three years on. CookieYes. https://www.cookieyes.com/blog/3-years-of-gdpr-impact/

Keepnet Labs. (2025, April 11). What is Security Awareness Training? *Keepnet Labs*. https://keepnetlabs.com/blog/what-is-security-awareness-training

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Laine, M. (2024). Preparing DevOps for ISO 27001 certification. Theseus. https://urn.fi/URN:NBN:fi:amk-2024121134618

Lanchec, S. (2024, April 19). *Access Control Best practices for Developers*. Forest Admin Blog. https://www.forestadmin.com/blog/access-control-best-practices-for-developers/

Levy, M., & Powell, P. (2004). Strategies for growth in smes : The role of information and information sytems. Elsevier Science & Technology.

Limited, D. (2023, October 5). *GDPR in a nutshell for the SME*. https://www.linkedin.com/pulse/gdpr-nutshell-sme-datatrust-limited/

McDowell, G. (2019, March 7). What does end of life mean for software and should you care? *Help Desk Geek - Tech Tips from Trusted Tech Experts*. https://helpdeskgeek.com/what-does-end-of-life-mean-for-software-and-should-you-care/

McIlwraith, A. (2021). Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness (2nd ed.). Routledge. https://doi.org/10.4324/9780429281785

Miller, M.(2024, June). Best practices for a culture of Security Compliance. https://auditboard.com/blog/best-practices-for-a-culture-of-security-compliance/

Modini, J., Lynar, T., Sitnikova, E., & Joiner, K. (2020). *Applications of Epidemiology to Cybersecurity*. Academic Conferences International Limited. https://doi.org/10.34190/EWS.20.057

National Cyber Security Centre Finland, NCSC-FI. (2020, February). Cyber security and the responsibilities of boards. https://www.kyberturvallisuuskeskus.fi/en/

National Cyber Security Centre Finland, NCSC-FI. (2022, August). Strengthening cyber security at Finnish organisations - Instructions for management and experts. https://www.kyberturvallisuuskeskus.fi/en/

Nepfumbada, J. (2017, April 24). Business Continuity Planning in the SME's. PECB Insights. https://insights.pecb.com/business-continuity-planning-smes/

Ohayon, H. (2024, April 8). The InfoSEC guide to the 10 types of information Security controls. Suridata. https://www.suridata.ai/blog/infosec-guide-to-information-security-controls/

Pandey, D. K., Prasad, S., Krishna, K. V. S. M., Saxena, S., Jani, V. (2022, December). An Assessment of Positive and Negative Aspects of Organisational Politics: A Systematic Literature Review on Psychological Wellbeing of Employees. Journal for ReAttach Therapy and Developmental Diversities. https://jrtdd.com/index.php/journal/article/view/117/99

Pansy. (2024, December 29). GDPR For Small Businesses: A Quick Guide For 2025. Sprinto. https://sprinto.com/blog/gdpr-for-small-companies/

Papathanasiou, A. , Liontos, G. , Katsouras, A. , Liagkou, V. and Glavas, E. (2025) Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era. Journal of Information Security, 16, 1-43. doi: 10.4236/jis.2025.161001.

Parlikar, S. (2022, October 3). A guide to SAAS Shared Responsibility model. *Revyz* . https://www.revyz.io/blog/a-guide-to-saas-shared-responsibility-model#:~:text=The%20SaaS%20provider%20will%20be,principles%20of%20least%20privileges%20and

Power, C. (2025, March 3). *The ultimate information security policy for small businesses | Power Consulting*. Power Consulting. https://powerconsulting.com/blog/information-security-policy-for-small-business/

Renvall, A. (2018). Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs. https://www.theseus.fi/bitstream/handle/10024/157277/Renvall_Aleksi_final.pdf?sequence=1&isAllowed=y

RichardMurphy. (2022, April 2). *Information security policies: why they are important to your business - Lantech Group*. Lantech Group. https://lantechgrp.com/information-security-policies-why-they-are-important-to-your-business/

Risk Ledger. (2022, August, 15) Are your organisation's information security policies accessible to all employees?. https://riskledger.com/da/support/framework/a/15

Rivera, A. (2024). A Small Business Guide to Computer Encryption. Business News Daily. https://www.businessnewsdaily.com/9391-computer-encryption-guide.html

Rüdell, I. (2025, March 18). *Importance of cybersecurity for small and medium-sized businesses*. Lumiun Blog. https://www.lumiun.com/blog/en/importance-of-cybersecurity-for-small-and-medium-sized-businesses/

Samira, N. Z., Weldegeorgise, N. Y. W., Osundare, N. O. S., Ekpobimi, N. H. O., & Kandekere, N. R. C. (2024). Comprehensive data security and compliance framework for SMEs. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2024.12.1.0146

Schell, E. (2015, February). Things to Consider When Purchasing a New System. Cyranesystems. https://www.cyranesystems.com/wp-content/uploads/2015/02/Purchasing-a-new-system_Schell.pdf

Schreider, T. (2019). *Building an Effective Cybersecurity Program, 2nd edition*. Rothstein Publishing.

Schwebius, P. (2024b, December 27). Cloud for SMEs – How to make the best choice? Lapala, the Human-centric Automation Platform. https://lapala.io/en/cloud-for-smes/

Shu, B. N. (2023, August 10). Navigating EDR Solutions: Open-Source vs. Paid — Choosing the Right Path. *Medium*. https://shublaisengwa.medium.com/navigating-edr-solutions-open-source-vs-paid-choosing-the-right-path-d2d58522dd00

Siitonen, T. (2020). INFORMATION SECURITY RISK MANAGEMENT - Ensuring the continuity of it in SMEs. https://urn.fi/URN:NBN:fi:amk-2020051811936

Soleman, D., & Soewito, B. (2024). Information Security System design using XDR and EDR. *Inform Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *9*(1), 51–57. https://doi.org/10.25139/inform.v9i1.7331

Spector IT. (2024, November 25). Anti-Virus and malware protection. https://www.spector.ie/services/cyber-security/anti-virus-malware/

Stabelin, H. (2025, March 21). *How to create an efficient access Policy: 7 key components*. Segura (Formerly Known as Senhasegura). https://segura.security/post/efficient-access-policy

Stasiak, A. (2022, October 4). Efficiency and Security: Implementing a Business Continuity Plan for SMEs. Startup-house. https://startup-house.com/blog/sme-business-continuity-plan-guide

Streefkerk, R. (2019, April 12). Qualitative vs. quantitative research | differences, examples & methods. Scribbr. https://www.scribbr.com/methodology/qualitative-quantitative-research/

Streefkerk, R. (2019, April 12). *Qualitative vs. quantitative research | differences, examples & methods*. Scribbr. https://www.scribbr.com/methodology/qualitative-quantitative-research/

Team, G. (2023, December 21). *Harnessing Security Patch Management for SME Defense - GXA*. GXA. https://gxait.com/business-strategy/harnessing-security-patch-management-for-sme-defense/

Thakral, A. (2022, January 21). *5 reasons why SMEs should use Cloud-Based services*. Target Integration. https://targetintegration.com/en_us/5-reasons-why-smes-should-use-cloud-based-services/

Thakral, A. (2022b, January 21). 5 reasons why SMEs should use Cloud-Based services. Target Integration. https://targetintegration.com/en_us/5-reasons-why-smes-should-use-cloud-based-services/

Timalsina, R. (2025, April 7). *5+ risks of using EOL software without support & security tips*. TuxCare. https://tuxcare.com/blog/end-of-life-software/#:~:text=EOL%20software%20no%20longer%20receives,attackers%20actively%20exploit%20unpatched%20vulnerabilities

TolaData. (2021, June 17). *Qualitative and Quantitative data collection methods in M&E*. https://www.toladata.com/blog/qualitative-and-quantitative-data-collection-methods-in-monitoring-and-evaluation/

Tovey, A. (2020, August 17). *Threat management: Endpoint Detection and Response Service*. https://tovey.net/endpoint-detection-and-response-service/

Trio Team. (2025, February 18). Enhancing Security: A comprehensive guide to device encryption. https://www.trio.so/blog/device-encryption/

Trust in Digital Life. (2018). GDPR-for-SMEs. https://trustindigitallife.eu/wp-content/uploads/GDPR-for-SMEs.pdf

Usercentrics. (2024, May, 21). Consent Management Checklist for GDPR Compliance. https://usercentrics.com/resources/gdpr-checklist/

Williams, N. (2018, November 7). Why SMEs Need a Secure Remote Working Policy . Fleximize. https://fleximize.com/articles/013434/secure-remote-working-policy

Appendices

Appendix 1. Survey questions whose details are explained in chapters 3 and 4

SQ7. Does your organization have its own documents and policies so that the employees can comply with the information security standards in order to prevent data breaches of sensitive and confidential information?
SQ8. Are the security policies at your organization reviewed and updated at regular intervals?
SQ9. Are the documented security policies at your organization easily accessible and understandable by the employees?
SQ10. Does your company have its own IT security training materials available for the employees to ensure that they know how to handle sensitive information?
SQ11. Are the GDPR guidelines at your organization followed while handling your clients/customers data?
SQ12. Where are your organization's data stored?
SQ13. Is the multi-factor Authenticator (MFA) enabled for all/part of the softwares used in your organization?
SQ14. When using any software for work purpose is it's security policy reviewed for GDPR purpose like where your organization 's data will be stored and what information will it gather?
SQ15. Do you organization have any automated way of obtaining the software Inventory if you are working globally?
SQ16. Does the antivirus software installed in your organization 's devices have malware protection capability?
SQ17. Are the endpoints or laptops provided by your organization encrypted?
SQ18. Are there any processes to handle the patches to take care of the various vulnerabilities where the critical security updates are managed centrally?
SQ19. Do your organization provide any remote working tool for secure remote access?
SQ20. Are there any business continuity plans documented and implemented for your organization?

Terminology:

AI	Artificial Intelligence
AV	Antivirus
BCP	Business Continuity Plan,
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
COVID-19	Coronavirus disease
DPO	Data Protection Officer
EDR	Endpoint Detection and Response
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
EOL	End of Life
EU	The European Union
GDPR	General Data Protection Regulation
ISC	Information Security Controls
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
MDM	Mobile Device Management
MFA	Multi-Factor Authentication,
MSP	Managed Service Provider
NDA	Non-Disclosure Agreement
OS	Operating System
PDCA	Plan-Do-Check-Act
PoLP	Principle of Least Privilege
PRISMA	Preferred Reporting Items for Systematic reviews and Meta-Analyses
RBAC	Role-Based Access Control
SaaS	Software as a Service
SBS	Small Business Standards
SIEM	Security Information and Event Management
SME	Small and Medium-sized Enterprise
SQ 7-20	Survey Questions 7-20
SSO	Single Sign-On
VPN	Virtual Private Network