UNIVERSITY OF TURKU
Turku School of Economics

ISO 27001 and Global Privacy Compliance

The Role of ISO 27001 in Emerging Privacy Frameworks in Europe, the USA and China

Report
Master's Thesis in Futures Studies

Author(s):
Asanka Ishari Wedeha Pathirana

Supervisors:
Markku Wilenius
Professor

31.05.2025
Turku

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check Service.

Table of Contents

Abstract

The global privacy regulations continue to evolve in complex and reach, organisations face increasing need to meet the expectation of the industry demands while maintaining robust security postures. This study aims to explore the role of ISO/IEC 27001 in emerging privacy compliance across three major jurisdictions —Europe (GDPR), the United States (CCPA), and China (PIPL). Through an empirical analysis and a theoretical framework developed around anticipatory governance, weak signals, and the legal nuances of privacy in the respective jurisdictions alongside ISO 27001, this study is leveraged to examine the evolving role of ISO 27001 in transnational privacy regulation. The research methodology of this study adopts a qualitative approach and uses thematic analysis based on 15 semi structured interviews with privacy and cybersecurity professionals from Finland, EU and the US. In the process of analysing the data , Nvivo software was utilised coding 668 references which was categorized in to 6 key themes reflecting operational, regulatory and strategic dimensions of ISO 27001's implementation. The findings from this study reveals that ISO 27001 provides a foundational security structure through the CIA principles (confidentiality, integrity, availability) and a risk based approach to the privacy governance. It was also noted that the foundational structure should be supplemented with privacy specific controls such as ISO 27701 and regeional adaptations to meet the regulatory obligations. It was discovered to comply with privacy legislation like the GDPR, CCPA, and PIPL, legal and organizational measures beyond ISO 27001's security architecture are needed for privacy related concepts like consent, data subject rights, cross-border transfers, and accountability. Emerging trends were also noted as future considerations that call for anticipatory governance and initiatives for continuous improvement, such as data localization and dangers associated with AI. The study contributes to the growing literature on global privacy compliance and highlights the importance of integrating security and privacy frameworks. It recommends that organizations adopt a flexible and forward-looking compliance posture that can accommodate regulatory volatility and technological innovation. Scenario trajectories discussed in this study—ranging from baseline convergence, to regulatory fragmentation, to a transformative global standard—offer a foundation for further foresight-driven analysis of ISO 27001’s evolving role amid privacy and AI governance pressures.

Key Words : anticipatory governance, CCPA, emergence, foresight, GDPR, information security, ISO 27001, PIPL, privacy compliance, thematic analysis, weak signals

Usage of the abbreviations

- **AI –** Artificial Intelligence
- **B2B** – Business-to-Business
- **B2C** – Business-to-Consumer
- **BCR** – Binding Corporate Rules
- **CCPA** – California Consumer Privacy Act
- **CIA** – Confidentiality, Integrity, and Availability
- **CIPP/E** – Certified Information Privacy Professional / Europe
- **CIPP/M** – Certified Information Privacy Professional / Management
- **DSR** – Data Subject Rights
- **EEA** – European Economic Area
- **EU** – European Union
- **GDPR** – General Data Protection Regulation
- **ISMS** – Information Security Management System
- **ISO / IEC** – International Organization for Standardization / International Electrotechnical Commission
- **PET** – Privacy-Enhancing Technology
- **PIMS** – Privacy Information Management System
- **PIPL** – Personal Information Protection Law
- **PbD** – Privacy by Design
- **SCC** – Standard Contractual Clauses
- **UK** – United Kingdom
- **US / USA** – United States of America

Chapter 1

1. Introduction

The rapid technological advancements have made organizations face uncertainty in the evolving business landscape. As technology advances, the regulations around it advance together to create a harmonious balance between innovation and compliance, ensuring that developments align with ethical and legal standards. Modern technology relies significantly on data, and it is important that the data is properly safeguarded to ensure privacy as well as security with the emerging regulations. Organizations that leverage emerging technologies are increasingly investing in strategic foresight capabilities to anticipate risks and enhance long-term resilience (Jissink, Rohrbeck, & Hölzle, 2014). One such industry standard that has been established to secure information security is ISO/IEC 27001. ISO 27001 is an Information Security Management System that provides a systematic framework to manage information security risks.

Organizations increasingly use foresight and anticipatory planning to prepare for regulatory changes (Pezzulo & Rigoli, 2011; Rohrbeck, 2012), and they adopt standards like ISO 27001 as proactive measures to manage evolving data protection requirements. While ISO 27001 focuses on enhancing data protection and resilience, Personal Data Protection, in other words, privacy, has gained attention as a fundamental human right. Regulations such as GDPR (General Data Protection Regulations), CCPA (California Consumer Privacy Act and China's PIPL (Personal Information Protection Law) have imposed specific requirements when dealing with personal data.

Organizations face increasing pressure to ensure their security controls prevent harm as regulations on privacy get more complex and widespread. Furthermore, many companies have invested in various security measures without systematically assessing their impact on privacy compliance, leaving a critical gap in the equation. This study aims to fill that gap by investigating how ISO 27001 enables an organization to meet privacy obligations and, finally, what most enterprises face in trying to make the framework fit into various privacy regulations. Through empirical evidence, the study intends to advance the understanding of how information security frameworks, such as ISO 27001, can be integrated into privacy

compliance strategies to heighten institutional accountability (Tikkinen-Piri, Rohunen, & Markkula, 2018).

1.1 Research and Questions and Objectives

This thesis is structured to answer three research questions. Each of the research question focuses on the relationship between the ISO 27001 and privacy compliance. These research questions aim to address different dimensions of ISO 27001's involvement in privacy and compliance process. The research questions and research objectivesare are as follows.

1.1.1 Role of ISO 27001 in Emerging Privacy Requirement

- **The primary research question is: What is the role of ISO 27001 in organizations in emerging privacy requirements?**
- **Research Objective: To determine the role of ISO 27001 in emerging privacy requirements.**

The first research question addresses how organizations perceive ISO 27001 as a tool for ensuring compliance with evolving privacy regulations. Key aspects include whether ISO 27001 has supported organizations in responding to emerging privacy regulations, which specific areas of privacy it addresses most effectively and whether the standard should be amended to better accommodate emerging privacy trends. This study aims to find answers to these questions by examining how ISO 27001 assists organizations in fulfilling privacy obligations, particularly regarding the rights of the data subjects, data minimization, and accountability. Further, it examines if the standard provides a strong foundation for privacy compliance. The insights from industry professionals will be analyzed to understand whether ISO 27001’s security controls align effectively with the privacy compliance requirements.

1.1.2 Supporting Privacy Compliance Across Regions

- **Research Question 2 – How does the implementation of ISO 27001 support compliance with privacy regulations across the regions?**
- **Research Objective - To explore how ISO 27001 supports compliance with regional privacy regulations.**

The second research intends to find how regional privacy requirements could be supported by ISO 27001, and this thesis aims to focus on the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the USA, and the Personal Information of Privacy Protection Law (PIPL) in China. Question number 2 specifically focuses on whether ISO 27001 facilitate these specific regional privacy regulations, If there are any notable differences in how ISO 27001 responds to these regulations, how to address gaps between ISO 27001 and the aforementioned regional privacy regulations and the sufficiency of the standard to address the emerging privacy regulations.

1.1.3 Challenges and Benefits of ISO 27001 in emerging privacy compliance

- **Research Question 3 – What Challenges and Benefits do organizations face when implementing ISO 27001 for emerging privacy compliance?**

- **Research Objective - To identify the key challenges and benefits of implementing ISO 27001 for privacy compliance.**

Research question 3 focuses on answering the potential challenges and benefits that organizations face when implementing ISO 27001 for emerging privacy compliance. This question seeks answers to identifying key challenges in implementing ISO 27001 in relation to privacy compliance and identifying the potential advantages a company could gain by achieving the ISO 27001 certification regarding privacy compliance. Further, this specific research question seeks answers on what organizational resources that are critical to successfully implement ISO 27001 in an organization and if there are any specific instances where ISO 27001 provided any measurable outcomes for privacy compliance.

1.1.4 Futures Perspectives on ISO 27001 and Privacy Compliance.

Apart from the three fundamental research questions, this study examines the future role of ISO 27001 on privacy compliance. As privacy frameworks are rapidly evolving and new technologies emerge, organizations must continually invest in future challenges that can anticipate and adapt accordingly. This exploratory section will examine experts' opinions and

ideas on how ISO might evolve with the changes in new privacy trends. Potential emerging trends and best practices that may come in future, the areas it may need to modify in its current state, and how to use ISO 27001 best amid the increasingly convoluted regulatory environment. Insights will also be drawn as to how organizations could make proactive efforts to align their security and privacy strategies toward future developments, as well as any advice from experts on ways of doing such.

1.2 Structure of the Thesis

This thesis is structured into five main chapters, and each chapter contributes to an overall understanding of ISO 27001's application in privacy compliance. The first chapter deals with the research topic and offers the questions and the objectives. Further, it explains the relevance of this research within future studies and ISO 27001 regarding Privacy Compliance, particularly in the context of how organizations predict and adapt to evolving privacy requirements. The second chapter develops the theoretical background to this inquiry by elaborating on the theoretical position that brings ISO 27001, information security, and privacy compliance together. It also expands to the concepts such as anticipation as well as emergence on relating the emerging privacy requirements; in the third chapter, the research design and methodology are discussed, which includes explaining the rationale for the qualitative approach chosen, semi-structured expert interviews employed during the study and thematic analysis. Moreover, there is information on the limitations of the research. The fourth chapter is devoted to the presentation of research findings, which were thematically organized to address each research question, including some other findings derived from industry experts. Lastly, the fifth chapter integrates findings from the research and discusses their implications for organizations while providing recommendations. Further, this study analyzes future views on ISO 27001 concerning privacy compliance by examining expert insights on data analysis. These findings, which consider potential developments and best practices of ISO 27001, are analyzed independently in the discussion chapter to highlight their implications on the future regulatory landscape.

Chapter 2

2. Research Design

There is a rapidly evolving legal landscape concerning privacy as well as personal data protection. However, ISO 27001's practical application, challenges and benefits, along with its role in personal data protection, are mainly outlined in this thesis. The research aims to achieve the main objectives: 1) to explore the role of ISO 27001 in helping organizations meet emerging privacy requirements and 2) to assess how ISO 27001 supports compliance with global privacy regulations across different regions. 3) to identify the challenges and benefits organizations face when implementing ISO 27001 for privacy compliance.

The primary focus of this thesis is to enhance the understanding and practices of ISO 27001 implementation for privacy compliance. Further, this thesis seeks to contribute fresh and new insight into the application of ISO 27001 in different global organizational contexts, specifically focusing on Europe, China and the USA. The primary data for this thesis has been collected through semi-structured interviews with selected privacy and cybersecurity professionals from different regions. This research intends to address the role of ISO 27001 in privacy compliance, its effectiveness in addressing the shortcomings in privacy compliance, and the advantages of ISO 27001 implementation for privacy compliance. The interviews will be supplemented by reviewing existing literature on ISO 27001 and privacy frameworks to contextualize the findings under more comprehensive terms.

After reflecting on the theoretical framework, the researcher decided that a qualitative approach would be more suitable for this study. The decision to adopt a qualitative research methodology stems from the unique nature of the qualitative method in relation to complex real-life organizational practices. This is consistent with the pragmatic research paradigm built in the applicability of research outcomes in real world scenarios. To preserve the theoretical openness no specific conceptual models or hypotheses were pre-established to be subject to deductive testing.

In this thesis, the pre-defined hypothesis was not established due to the exploratory nature of the research. Hypotheses are usually used in deductive research where existing theory is

deliberately tested through structured methods. However, this thesis will deal with how ISO 27001 has a role in privacy compliance, what difficulties organizations face, and other benefits that may be gained in its implementation. There is very little prior research in this area. Due to this complexity and variety of organizational actions across the world, a rigid hypothesis-based approach could hinder further findings. Instead, an open-ended qualitative method permits a more nuanced view of real-life experience, thus finding trends, thematic elements, and new perspectives that do not necessarily have to relate to a preconceived assumption.

The foundation of qualitative research is the idea that people derive meaning from their interactions with their surroundings. Creswell (2013). Additionally, a thorough examination of practitioners' viewpoints and experiences with ISO 27001 implementation yields valuable insights into how businesses handle privacy compliance issues. Qualitative data provides a broad, comprehensive and multi-dimensional understanding that transcends numerical analysis, making researchers determine the complex patterns or themes that may emerge from the research topic (Denzin & Lincoln, 2005).

According to Denzin and Lincoln (2000), a research paradigm is a specific set of presumptions and concepts that aid in the interpretation and resolution of complex real-world problems. It will also affect the methods of data analysis that are used and the research approaches that are chosen. This thesis adopts the framework of the pragmatic research paradigm, which places importance on practical solutions and applications in the real world. Fundamentally, pragmatists perceive knowledge to be the byproduct of human experience in life and value only those life experiences that contribute to broadening their understanding (Kaushik & Walsh, 2019). This applies to the objectives of the current study, advising the organizations on the best methods for the application of ISO 27001 to realize privacy compliance. The following section discusses the research paradigm and data collection methods developed for the study.

2.1 Research Methodology and Data Collection

The data collection for this thesis was primarily based on the output of semi-structured interviews. The semi-structured interviews were extensive, and there has been a total of 15

participants in the research data analysis in the coming chapter. The semi-structured interview method was chosen for this study since it allows flexibility of participants, allowing their perspectives to be heard well according to a question set that was made per the research questions and objectives. This approach also enables the researcher to adapt the interview process based on the responses provided, ensuring that emerging themes and unanticipated topics can be explored in detail (Kvale & Brinkmann, 2009)

The researcher had considered using the literature review as a combination with the 15 experts for the data collection; however, after careful consideration, the researcher decided due to the extensive nature of the interview output as well as the limited resources written on the emerging and future perspective of the ISO 27001 and privacy compliance, the data collection and analysis will be done through the insights gathered from the experts. Since the study depends exclusively on the 15 expert interviews, it is feasible to get in-depth insight from those actively involved in privacy compliance so that the conclusions indicate what organizations confront in practice. This makes for a more direct investigation of issues and benefits associated with ISO 27001 and privacy compliance in real life, which often have not yet been fully caught in the literature.

To avoid over-reliance on a limited number of experts and to ensure a diverse range of perspectives, 15 experts were interviewed to enhance the accuracy and reliability of the findings. Initially, it was suggested that the interview participants should be 12. However, a larger group of fifteen specialists was chosen to guarantee rich and varied feedback. Semi-structured interviews were performed online and in the interviewees' various offices between May and August 2023. The interviews were scheduled in a one-hour slot. However, four interviews took an average of 45 minutes; 5 interviews, each averaged around 75 minutes; and the remaining six interviews lasted about an hour. Further validation and refinements were made through 3 sparring sessions with experts and practitioners in the field.

Initially, 17 interviews were conducted to gather data for the thesis. However, though 2 of their responses were later regarded as void, this was because the quality of the interviewee's insights was not sufficient and proved neither to have actively contributed to the process of implementation of the ISO 27001 standard in their respective work experience. The focus of the neglected interviewees was mostly on legal views as opposed to their actual application within organizations, which was the primary objective of this study. The main research

question is to find the role of ISO 27001 and how it can be integrated into privacy and compliance; those inputs did not meet the research focus. Therefore, the final analysis does not include these two interviewees, leaving 15 expert interviews for data analysis.

The interview questionnaire for this study (Appendix 1) was prepared before the interviews. Each interviewee was sent details on the rights of the interviewee along with the data protection statement (Appendix 2 and 3), how to answer questions and an extensive data protection declaration prior to the interview. While it was not expected to prepare for the interviews, those who wished to do so were given that opportunity by sending the interview questions beforehand. The questionnaire was employed flexibly during the interviews, with questions amended or omitted according to relevance for each participant without affecting the intergrity and the research objectives. Interviews were conducted using Microsoft Teams and physically at their work premises to allow for the recording of the discussions. After the meetings, Teams transcribed the sessions, and the researcher reviewed and edited these transcripts prior to further analysis. Every interview was conducted in English, irrespective of the participant's mother tongue. The author used Microsoft Teams and a tool called otter.ai to transcribe the interviews. However, a few interviews had to be transcribed manually due to the different pronunciations. Further, each interview was manually checked for accuracy. The researcher further accepts responsibility for any misinterpretations or inaccuracies arising from the transcription of the analysis.

2.1.1 Interview Participants

In this study, the interviewees were found and contacted through LinkedIn, a professional social networking platform. Due to the wide range of connections made by the researcher in the area, inviting prospective interviewees and securing their participation was a relatively smooth process. Initially, 20 invitations were sent by the researcher to professionals whose LinkedIn portfolios showed relevant experience in ISO 27001 implementation and privacy compliance. Of these, 17 accepted the invitation to participate, and finally, 15 were included in the final analysis once it was ensured that their contributions aligned with the study's objective.

The selection criteria were based on the job descriptions, their work experience, and the experience they had in ISO 27001 implementation at either their current or past organizations.

In fact, at least 80 per cent of the final interviewees had professional certifications in personal data protection, a qualification widely accepted in the field. This endorsement ensured that the researcher was engaging high-quality participants, which also increased the chances of obtaining insightful and reliable data for the study.

The researcher ensured that the participants had worked at least the implementation stage of ISO 27001 in their respective organizations. The Participants held various positions in their organizations. The positions included privacy professionals, cybersecurity professionals, consultants, and professors. These participants represented their organizations, and those organizations were preliminary multinationals. Participants were situated in the European Economic Area and the United States. The thesis focuses on the regional data protection laws of Europe, the USA (CCPA), and China. Even though the participants were not from China, most of them demonstrated that their respective organizations do operations with China. The researcher attempted multiple times to reach consultants situated in China. However, none of the potential participants agreed to participate in the research. However, the researcher collected the data from the participants who agreed and worked with Chinese data protection regulations.

All research material is anonymized in this thesis. All published materials are anonymized, and it was informed at the data collection that no personal data will be released during data analysis or discussion. These decisions were made to maintain the integrity and transparency of the research. Personal data protection, in other words, "Privacy", was paramount to the author. These boundaries were respected during the thesis's process. Interviewees are referred to as "Participants", and each participant was given a number. In the data analysis, the Participants are also referred to as "Interviewees". (Refer Table No 1)

Table 1. Overview of Interview Participants

Participants	Industry	Position	Location	Market Reach
Participant 1	Finance	Privacy Professional	Former EEA member country	Global

Participant 2	Industrial Technology	Privacy Professional	EU	Global
Participant 3	Professional Services	Consultant	EU	EU
Participant 4	Telecommunication	Privacy Professional	EU	Global
Participant 5	Professional Services	Consultant	EU	Global
Participant 6	Telecommunication	Privacy Professional	EU	Global
Participant 7	Information Technology	Privacy Professional	EU	Global
Participant 8	Professional Services	Privacy Professional	USA	USA
Participant 9	Information Technology	Cybersecurity Professional	USA	Global
Participant 10	Technology	Privacy Professional	EU	Global
Participant 11	Professional Services	Professor	Former EEA member country	Global
Participant 12	Information Technology	Cybersecurity Professional	USA	Global
Participant 13	Technology	Cybersecurity Professional	EU	Global
Participant 14	Technology	Privacy Professional	EU	Global
Participant 15	Technology	Cybersecurity Professional	EU	Global

2.1.2 Interview Questions

The interview has sections that are supposed to obtain different insights from the participants. The first part of the interview questions is to learn about the interviewees' backgrounds, their professional roles, and their involvement in the implementation of ISO 27001. The second part of the question is on organizational context: how the systems of privacy compliance and information security management systems (ISMS) were incorporated within their companies. The third part consists of questions on regional differences in different regulatory landscapes, and the fourth part is on the challenges and the benefits of ISO 27001, specifically relating to privacy and compliance. The fifth and final part is specifically added to gather expert insights on the future perspective of ISO 27001's involvement in personal data protection.

Semi-structured interviews with industry experts in privacy and cybersecurity formed the basis for the empirical findings of this study. A semi-structured interview method was used to allow consistency in data collection while remaining flexible for new insights. Giving respondents the freedom to elaborate on their experiences in the process made sure that a nuanced and in-depth output could be received. Follow-up questions helped create a deeper, more open conversation as important topics came up during the interviews. Open-ended questions also gave participants the chance to share their thoughts more freely. Using semi-structured interviews worked well for gathering detailed insights on how ISO 27001 is implemented, how organizations handle privacy compliance, and what challenges or opportunities they see for the future. The mix of structure and flexibility made this approach especially useful.

2.1.3 Data Analysis

This section presents the methodology chosen for the data analysis. The interview data were subjected to thematic analysis. It is one of the most employed qualitative methods which deals with identifying the patterns and themes within the data. This was important to identify the commonalities and contrasts in participants' experiences vis-à-vis ISO 27001 implementation and privacy compliance, thus leading to a richer understanding of the research issue (Braun & Clarke, 2006).

Data analysis, inductive or deductive, refers to orientations set about by Braun & Clarke (2022). With inductive analysis, themes emerge from the data themselves in real-time without any predefined framework, while deductive analysis has existing theories and research questions that guide the coding. This study utilized both deductive and inductive approaches, whereby deductive coding ensures the data relate to the general objectives of the study, whereas inductive coding allows for the emergence of themes from the participants' insights.

NVivo is qualitative analysis software that aids the data analysis process by organizing, coding, and managing the qualitative data. The author found NVivo ideal for systematically categorizing the interview responses and therefore provided for a structured and rigorous analysis of the views of privacy and cybersecurity professionals toward ISO 27001. The Chapter 4 consist of the more elaborative chapter on the data analysis that was gathered by using NVivo analysis.

The excerpts from the interviews that were included in this thesis have been subjected to careful editing to protect the confidentiality of the interviewees and the privacy of their organizations. Names of persons, places, or other identifiers relating to administrative regions and organizations were changed or removed so that no individual or entity could be identified in any way. The changes to the interviews were made entirely for reasons relating to confidentiality and did not interfere with the actual content or the integrity of the responses. The content mirrors the intentions and viewpoints of the participants, faithfully reflecting on what they really presented.

2.1.4 Thematic Analysis

The thematic analysis (TA) method was basically chosen as the data analysis mode for this research. Theme analysis is one of the most used methods. This is aimed at allowing researchers to identify, analyze, and interpret patterns or themes within qualitative data without being bound to a particular theoretical framework. The flexibility of the thematic Analysis makes it easily applicable to a broad spectrum of research questions in different sample sizes and diverse data collection methods (Clarke & Braun, 2017). This creates a perfect match for the aims of the thesis.

Thematic Analysis can also works well for researchers learning about qualitative Analysis, such as the author of this dissertation, as a structured but open analytic approach.

The study was, however, guided through the six phases of thematic Analysis as proposed by Braun and Clarke (2022):

Table 2. Six Phases of Thematic Analysis

Phase	Description
Phase 1- Familiarizing Yourself with the data	In the first phase, a researcher gets an in depth familiarizing by spending time with the data, listening to the interviews, reading and re-reading the transcripts, and writing down any ideas that come to mind. Braun and Clarke (2006) propose that thematic analysis considers representation of data such that all its nuances are understood.
Phase 2 - Coding	In Phase 2, relevant segments of data were identified and meaningfully labeled with codes. The coding was done on a spectrum ranging from explicit (semantic) intent to one with more implicit (latent) connotation. The specific objective of this phase was to categorize the data in such a way as to promote access for further analysis.
Phase 3 – Generating Initial Themes	The third phase entails the patterning and meaning making of the data by the researcher. Core concepts and/or ideas shared by the related codes and research questions were grouped to create main themes. This step focuses on constructing themes from the data, the research questions,

	and the researcher's insights, with themes representing shared meanings and codes referring to specific instances of those meanings.
Phase 4 -Developing and Reviewing Themes	In the phase four candidate themes were critically reviewed to ensure they accurately represented the data. The researcher worked through the themes regarding their relevance from coded excerpts to their full data set. Then, the themes were split and joined or tested for elimination to produce the best theme to capture the 'most significant reflections ' corresponding to research questions. This phase was the clear articulation of the central organizing idea of each theme.
Phase 5 - Refining, Defining, and Naming Themes	In the fifth phase, the specificities of each theme were refined such that every theme was unambiguously defined and accorded with the objectives of the research. An appropriate name was assigned to each theme to reflect the essence of the content it represented.
Phase 6 - Producing the Report	The last phase of the thematic analysis was the initiation of an analytic narrative. This was made entertaining with the use of data extracts to signify the themes' relationship to the research questions. These really were moments where writing would have significantly influenced the entire process, assisting with ongoing analysis and refinement of the outcomes.

Adapted from Braun & Clarke (2022)

2.1.5 Potential Limitations of the Research

This research is conducted mainly using qualitative methods. Hence, it is crucial to critically overview the scope, credibility, and ethical issues surrounding it. Several areas influence the reliability of the research: choice of interviewees, research methodology, and subjectivity in interpreting data. Credibility requires transparency and openness concerning matters where established literature or standardized frameworks may be lacking. This section assesses other ethical concerns relating to the research issue, including issues concerning the researcher's role, limitations and data analysis.

In this study, one significant limitation is the varied interviewees' different interpretations of the concepts of privacy and cybersecurity compliance. While all participants are experts in their own domains, their individual perspectives on the implementation of ISO 27001 and on the challenges of compliance therein may vary due to their own regional setting and their own organizational context. This presents a potential risk of subjective biases and different definitions. The impact of this risk was minimized through the construction of open interview questions that allowed for follow-up clarifications. Nevertheless, divergence in terminology and practical experience between the researcher and the interviewees may still act as potential sources of misinterpretation.

Further, there is a geographical limitation in the sense that there are European and US experts in this study that may not capture any global variations in implementing ISO 27001. The research question especially includes China, and the absence of an expert based in China could potentially affect the analysis since the expert's opinions are based on those participants who are situated outside China. The respondents work in multinational organizations; however, the insights they provide are subject to regulatory environments pertaining to their own countries. Thus, this limitation indicates that the present study does not compare or rank different compliance approaches across jurisdictions and only seeks to illustrate current practices and challenges in the industry. Despite these limitations, it nevertheless provides useful insights into how ISO 27001 is used for privacy compliance in different organizations.

It is worth noting that the study has few limitations that may affect the scope and applicability of its findings. For example, whilst the interviewed professionals gave valuable perspectives, their perspectives might not be wide enough to cover the whole field of implementation of ISO

27001 across different industries and organizations. Secondly, the present study was quite focused on ISO 27001 while not paying attention to the other standards, like NIST or SOC 2, which may be very important in terms of cybersecurity and privacy compliance.

In addition to this, the rapid change in the regulatory environment means that although the findings may reflect compliance practices at the time of the research, future changes in legislation may obscure this information. Other limitations arise due to some of the interviews being semi-structured, resulting in response variation based on follow-up questions. The lack of direct organizational data, too, made the study rely on the expert's opinions rather than internal compliance documentation or audit reports, which otherwise would have added a better perspective.

Potential limitations and biases that might influence the research are acknowledged by the researcher. The researcher had solid experience in compliance. However, they had limited experience in qualitative research, including semi-structured interviews and thematic analysis. As a solution to this, the researcher sought preparatory efforts, which included reading literature, consulting with experienced professionals, and studying formal qualitative research methodologies. Further, in semi-structured interviews, participants asked follow-up questions for clarity, which may unintentionally influence responses. To mitigate this, the researcher was cautious about using neutral phrasing to avoid this potential influence.

The researcher was a professional in the field that is relevant to this study, which was another important factor to consider, as this could have introduced personal biases into the interpretation of the results. By keeping a reflexive journal during the research process, where all personal reflections and potential influences on the study were recorded, the researcher aimed to lessen some of these biases. The researcher also systematically followed a structured reflexive thematic analysis that considered rigour and reliability in data analysis. Transparency and critical reflection allowed the researcher to preserve the integrity of the findings, even if subjectivity is an inevitable part of qualitative research.

2.1.6 Organizational Collaboration in Research

The research for the publication was primarily conducted while the researcher was employed as a thesis worker at a technology company in Finland. The researcher, as an internal employee,

received a salary as a part of the company's ordinary payroll system. Due to the employment, the researcher has access to the respective company resources, which allowed the researcher to see deeper into the history and other ISO-related certification processes of the company. Regardless of being an internal employee, the researcher requested full independence for the research, which was agreed by the company. The investigation was not, therefore, influenced in terms of design, methodology, or results by the company, maintaining full transparency and academic integrity. The integrity of this research was strongly protected in the sense that the researcher maintained full control of the whole data collection and analysis process, while the company merely fostered an environment for the conduct of the research, hence providing no input as to what the specific priorities of this work should be or what the ultimate results of the work should look like. This ensured that research findings remained unbiased, credible, and trustworthy.

While researchers had complete autonomy during the research, the primary objective of the company was to analyze the aspect of ISO 27001 as applied to privacy compliance, as well as how an ISMS could serve to advance and enhance its compliance regime. The study, therefore, aligned with the company's interest in using ISO 27001 to bolster internal structures and appeal to evolving regulatory requirements. Although the study had considered these interests, the researcher was keen on maintaining an industry view by including the perspectives of participants who are working in other companies outside the company and not merely focusing on internal employees. This enabled a good balance between the comprehensive analysis of both the academic and professional requirements.

2.1.7 Role of the researcher

Being an internal employee with access to the company's resources, the researcher could also conduct three additional interviews with other employees of the company who are closely working with ISO standards such as ISO 9001 and ISO 14001. These interviews were expected to give an insight into the process of gaining and maintaining ISO certifications from a much broader operational dimension in the corporate environment. Such insight into the practical implications and governance of these standards assisted the researcher in setting up a more holistic visualization of how ISO 27001 could fit into privacy compliance initiatives. This additional information, therefore, complemented the primary research findings by

contextualizing ISO standards within a larger framework of corporatization practices relating to standardization, thus deepening the overall analysis in the study.

For an effective study it is necessary to disclose the researcher's background, biases, and methodological flaws. According to Lincoln and Guba (1994), an individual's positionality influences how knowledge is formed. Hence it is argued that one must be aware of and consider one's own biases and viewpoints at every stage of the research process. Similarly, Creswell and Poth (2018) pointed out that reflexivity is significant in qualitative research; thus, a researcher must consider how his or her own background and assumptions affect data collection and interpretation. By so doing, this study guarantees transparency and methodological integrity throughout the process.

Although the researcher was unfamiliar with ISO 27001 in the academic sense, they upgraded their knowledge through professional experience, courses on technology law on privacy and continuous learning from industry updates on platforms like LinkedIn. Minor studies in the faculty of law at the University of Turku provided a strong sense of understanding of regulatory frameworks and compliance mechanisms, which are also necessary for analyzing the interrelation between ISO 27001 and privacy regulations. The researcher acknowledges the potential impact of personal experience and has taken steps to maintain objectivity. Competing perspectives of different professionals in the industry have been brought into the analysis as a reflexive research approach and careful transparency in coding decisions. Such measures would make the study a rigorous and credible one while still recognizing the limitations that the researcher.

Chapter 3

3. Theoretical Framework

The Theoretical Framework consists of a well-organized and interconnected set of concepts and assumptions drawn from one or more theories that a researcher constructs a support study. In developing a theoretical framework, the researcher should outline relevant concepts and

theories to form a research foundation, establish logical connections between them, and link these concepts to the ongoing study (Grant & Osanloo, 2014). This chapter provides an overview of the existing literature written on the context of the research to build a strong theoretical foundation. In the process of doing so, the topic shall be divided into small parts to define what it means by each section of the topic. The theoretical background revolves around a collection of different theories. However, the connection and interlink between each of the theories are presented in the subsequent chapters of this section.

3.1 Emergence in Global Privacy Frameworks

Emergence has long been studied in philosophy and systems theory. Meehl and Sellars (1956) describe emergence in terms of different kinds of change, such as chance occurrence, systemic shift, and cumulative change, highlighting how new properties can arise unpredictably from complex interactions. According to their study, there are three kinds of change: Chance Occurrence, Shift and Cumulative Change (Meehl & Sellars, 1956). Emergence has been used in many scientific literature in various fields. "*Emergence is ubiquitous"* (de Haan, 2006).

Emergence is the reason to establish systems. Emergence refers to the process by which complex systems or phenomena arise from the interaction of simpler elements, often in ways that are not immediately predictable from the properties of those individual components. In many fields, this can be seen as how properties behave collectively in the form of a system. This results in a novel outcome, and it is extremely difficult to offer credit for the contributions made by individuals alone. Emergence has its applications in systems theory, sociology and many other areas.

In the context of global privacy regulation, emergence can be understood as a complex adaptive system, which is a core concept in futures studies that is applicable in systems composed of diverse and interacting agents capable of adaptation and self-organization (Holland, 1992; Miller & Poli, 2010). Personal Data Protection regulations as GDPR, CCPA and PIPL and information security management systems such as ISO 27001 do not develop in silos but evolve through the iterative interactions between regulators, industries and technologies. These interactions produce emergent regulatory patterns that cannot be reduced to the sum of individual components. ISO 27001 operates within this adaptive system by offering a flexible

and structured response to shared concerns over personal data security, facilitating the capacity of the system to evolve under uncertainty. This shows how legal and technical instruments coexist and co-evolve to meet the demands of rapidly changing digital environments.

Legal systems provide consistency and justice in legal decision-making by setting fundamental guidelines controlling compliance, culpability, and rights (Craig & De Búrca, 2021). In a legal context, a framework is defined as a structured system of laws or principles that guide the interpretation, implementation and enforcement of legal provisions in a specific domain. The International Organization for Standardization defines a framework as a structured approach that provides a foundation for designing, implementing, or assessing procedures, concepts, or technologies supported by best practices, guidelines, and tools (International Organization for Standardization, 2018).

3.2 Privacy Frameworks: A Legal Perspective

3.2.1 Historical Foundations of Privacy

Privacy is a concept that has many meanings. The definitions that can be given for Privacy can even be different from country to country or discipline to discipline. Further, what is Private and what is legally protected as "Private" can differ (Konvitz, 1966). According to the well-known writers Louis Brandeis and Samuel Warren in 1890, the Right to Privacy meant 'the right to be let alone'. Since then, the recognition of Privacy has emerged as a fundamental human right in the European Union. Privacy has remained a subjective concept even though social views may vary around the globe due to a failure to define what it means.

Although frequently mistaken for one another, privacy and data protection have distinct conceptual meanings. Privacy is a fundamental right regarding personal autonomy, whereas data protection is a regulatory framework meant to practically safeguard personal data (González Fuster, 2014). In this study, the term "privacy" serves as a larger legal umbrella under which 'personal data protection' acts as an operational mechanism, especially in those jurisdictions that have bound the two legally, as in the case of the GDPR. (Bygrave, 2010). Nonetheless, the researcher understands the overlap between the right to Privacy and the right to data protection. However, the goal of this study remains privacy from a legal perspective, and in a broader sense, "personal data protection" is primarily referred to as "privacy."

3.2.2 Privacy as a Human Right in International Law

"Article 12 of the Human Rights Declaration states that

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
(Council of Europe/European Court of Human Rights, 2022)

Other than Article 12 of the Universal Declaration of Human Rights (United Nations, 1948), Article 17 of the International Covenant on Civil and Political Rights (United Nations, 1966), Article 8 of the European Convention of Human Rights (Council of Europe, 1950), and Article 7 of the Charter of Fundamental Rights of the European Union (2000) also mentions the similar definitions. Everyone has the right to have their private and family life, home, and correspondence respected, as well as the ability to defend themselves against such unlawful interference.

3.2.3 The Emergence of Data Protection and Modern GDPR as a Legal Framework

When computers first appeared in the 1970s, many began to wonder if the right to privacy might also ensure the protection of private life. As a result of this technical advancement, a new right known as the right to data protection emerged. European General Data Protection Regulations (GDPR) was established in 2018 as an attempt to protect personal data.

The GDPR sets out basic principles and rights aimed at protecting personal data in the EU. Along with minimization, accuracy, integrity, and confidentiality, it also highlights the principles of lawfulness, fairness, and transparency (Regulation (EU) 2016/679, Art. 5). Regulation (EU) 2016/679, Art.12-23, further grants individuals several rights, such as access, rectification, erasure (right to be forgotten), restriction of processing, and data portability, which gives them control over how their data is used. Organizations must also designate a Data

Protection Officer (DPO) for supervision, perform data protection impact assessments (DPIA) where necessary, and implement data protection by design by default (Regulation (EU) 2016/679, Art. 25, 35, 37). This principle, articulated in Article 25, obliges organizations to embed privacy measures into the design of systems and processes from the outset and to ensure that, by default, only data necessary for each purpose is processed. EU Regulation 2016/679, Article 30, 34 states that there must be a record of processing activities (RoPA) and notification of data breaches to authorities and affected parties. These duties and principles further transmuted into an elaborate layout for privacy compliance that organizations must follow to secure the personal information and safeguard the rights of individuals.

The GDPR's Article 32 addresses the security of personal data and establishes a clear connection between privacy protection and security measures. Encryption and pseudonymization are just two examples of the technological steps that data controllers and processors should put in place to safeguard the level based on the risk. Therefore, the conclusion may be drawn that privacy rights should be protected, with the very primary consideration being personal data confidentiality, integrity, and availability (GDPR, Art. 32(1)). With the emphasis on security under the regulatory framework of the GDPR, privacy risks are mitigated since every security breach can cause grievous infringement of privacy, specifically in the context of Article 32(2), which highlights the necessity for testing these measures regularly (GDPR, Art. 32(2)).

3.2.4 CCPA and the United States of America (USA)

The privacy legal landscape in the United States is a complex system of federal, state and sector-specific laws rather than a single comprehensive framework. Key federal laws include the Health Insurance Portability and Accountability Act (HIPAA), which protects personal health information. Gramm-Leach-Bliley Act (GLBA) is also another significant act focusing on the security of the financial data. At the state level the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Act (CPRA) have new standards for data privacy by granting consumers rights such as data access, deletion, and opt out of data sales. These laws require businesses to implement stringent data protection measures and offer transparency in data processing activities ((Schwartz & Solove, 2021). The patchwork of privacy laws in the US poses challenges for organizations operating in multiple jurisdictions,

increasing the need for adaptable security frameworks that align with diverse legal requirements (Cate, F. H.,2020). This thesis focuses generally on USA since the complexities of the legal landscape is too wide to address. The researcher aims to address the USA legal landscape through the data collection mainly from the perspective of the industry experts who has worked with the stakeholders in USA- California and for the scope of this study, the focus from the USA privacy laws, California Consumer Privacy Act (CCPA) only was taken into consideration.

ISO 27001 is an international standard for information security management systems, and it provides a framework for organizations to manage and protect sensitive information. This framework provides Organizations in USA with structured methods to address privacy and security obligations under this fragmented legal environment. Establishing an Information Security Management System helps organizations implement risk-based controls to secure sensitive data and comply with regulatory requirements such as HIPAA's technical safeguards and the CCPA's data protection mandates. For instance, Annex A controls in ISO 27001—like A.10 (Cryptography) and A.16 (Incident Management)—help meet the encryption and breach notification requirements stipulated by these laws (ISO/IEC, 2022). Implementing ISO 27001 also demonstrates a commitment to international best practices, enabling U.S. organizations to build consumer trust while ensuring compliance with both domestic and global privacy regulations (Peltier, 2016).

Even though in the European Union, Privacy is a Fundamental Right, the United States has a different take on Privacy. Privacy cannot be found within the scope of the Constitution nor the Bill of Rights (Richards, N. M. (2013). The First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments are the Constitution's earliest sources of the right to privacy inferred by the Supreme Court. In In *Whalen v. Roe (1977)*, a case in which the Constitution recognized two main elements of privacy - the right to personal matters and the right to make weighty decisions without external interference - privacy became, for the first time, an informational perspective on the right recognized by the Supreme Court.

3.2.5 China and PIPL

On Nov. 1, 2021, China enacted the Personal Information Protection Law (PIPL) and thus began a significant step in the development of data protection and privacy rights in mainland China. Alongside other principles fairness, necessity, and transparency the law, emphasize lawfulness by requiring explicit legal grounds for processing personal data (Wang, 2021). One of the strictest components of the PIPL concerns cross-border data transfers: organizations must conduct security assessments and often seek official certifications before exporting personal data (Liu & Lin, 2022). These controls present China's approach for fortifying its national data sovereignty and keeping sensitive data within its territory. One could argue that other than the geopolitical strategies, PIPL has some commonalities with the EU's General Data Protection Regulation. However, PIPL puts a stronger inverse emphasis on explicit consent as the precondition for processing personal data than the General Data Protection Regulation (GDPR) itself, which allows data processing based on legitimate interest ((Greenleaf, 2021; Wang, 2021). This means that organizations under PIPL must seek unambiguous and affirmative consent from individuals before they can collect or process their personal information, making compliance significantly stricter than under the GDPR framework.

3.3 GDPR, CCPA and PIPL Relevance to Data Protection and Security

Compliance requirements under GDPR, CCPA, and PIPL enhance the coverage of privacy and data protection while keeping in mind their different regional focuses and operational implications. It provides clarity concerning Articles 5, 6, and 7 of the GDPR concerning the principles of lawful processing, consent, and transparency in safeguarding individuals' rights to their data. These include the rights to access, rectification, erasure, and restriction of processing, which are the principal aspects of organizational compliance (Regulation (EU) 2016/679, Art. 15-22). Further, the organizations within the territorial scope of the United States analogously provide for the CCPA (Cal. Civ. Code § 1798.100 et seq.) and the CPRA (California Privacy Rights Act) which is the amendment of CCPA with stronger preferences of granting consumers the rights of requesting access to and deletion of their data, to deter the sale of such data to third parties (Cal. Civ. Code § 1798.120). ISO 27001 controls strengthen these measures by A.13.2 (Protection of Personal Data) and A.9.2 (User Access Management) to enable organizations in both jurisdictions to secure their data. PIPL in China lays down

stringent consent requirements on data processing under Articles 13 and 14, which require 'unambiguous and genuine informed consent' by an individual before processing that individual's data (Liu & Chen, 2024). It also allows the assessments for security consideration of cross-border data transfers as per Article 38, reflecting China's strict data sovereignty.

3.4 Comparative Trajectories of Emerging Privacy Frameworks

It is important to understand the ongoing divergences in global privacy regulations, as they offer insight into the possible future directions and interactions these frameworks may take (Greenleaf, 2021). While the GDPR, CCPA, and PIPL are all regulations that were formed by different parts of the world for protecting personal data, they constitute different regulatory logics conditioned by the region's values and political systems (Kuner et al., 2020). For example, GDPR does not prevent multiple lawful bases for processing, such as legitimate interest (GDPR, Art. 6(1)(f)); yet the PIPL from China has a stricter model which requires, in most cases, an explicit and fully informed consent (PIPL, Art. 13–14). Conversely, CCPA uses an opt-out model, focusing on sales of data, in which user options are emphasized mainly after the collection of data (CCPA, §1798.120).

The enforcement structures are also very much different: the GDPR is implemented through Data Protection Authorities based in individual countries, with coordination from the European Data Protection Board (EDPB) (GDPR, Art. 68–70); the CCPA centralizes authority in the California Privacy Protection Agency which is also equipped with the powers to grant civil fines (CPRA, §1798.199.10); and PIPL conferred huge powers on the Cyberspace Administration of China (CAC), reflecting a more state-centered type of control (PIPL, Art. 60). All three regulations claim extraterritorial reach yet the mechanisms and conditions for enforcement vary, thus creating legal uncertainty for cross-border data flows (Bradford, 2020).

The divergence of regulatory authority is further highlighted by the dissimilar governance models—from the multilateral coordination of the European Data Protection Board (EDPB) to the independent oversight of the California Privacy Protection Agency (CPPA), the regulatory body established by the CPRA to enforce California privacy laws (CPRA, §1798.199.10), to the centralized enforcement of the Cyberspace Administration of China (CAC). These contrasts exist not only to mirror a fractured present but also to determine possible futures for global

privacy governance, suggesting that pressures for harmonization and geopolitical tensions might weigh on the development of more interoperable, adaptable standards (De Hert & Papakonstantinou, 2012). In this view, frameworks such as ISO 27001 may be taken to provide anticipatory instruments to manage such complexity by aiding alignment across jurisdictions without requiring legal uniformity (Shaffer & Pollack, 2010).

3.5 ISO 27001 and its history

Determining how evolving privacy frameworks relate to ISO 27001 requires an understanding of the standard and its history. National standards organizations around the world contribute to the International Body for Standardization (ISO), an independent non-governmental international body that creates international standards. The prerequisites for setting up an information security management system (ISMS) are its focus. It is the primary standard recognized by ISO for Information Security. The objective of this security framework is to safeguard a company's information systematically and efficiently, regardless of the organization's size or the sector (Bughin, Chui, & Manyika, 2013).

The adoption and certification of Management systems international standards such as ISO 9001,14001 and ISO 27001 have achieved significant global recognition, with over one million organizations having certified quality management systems. (Kaur, Kochhar, Ganguli, & Rajest, 2021). The concept of ISO 9000, which focuses on quality management systems, has been around for more than 30 years, and initially it was not expected to be embraced by such many organizations across the globe (Buttle,1997).

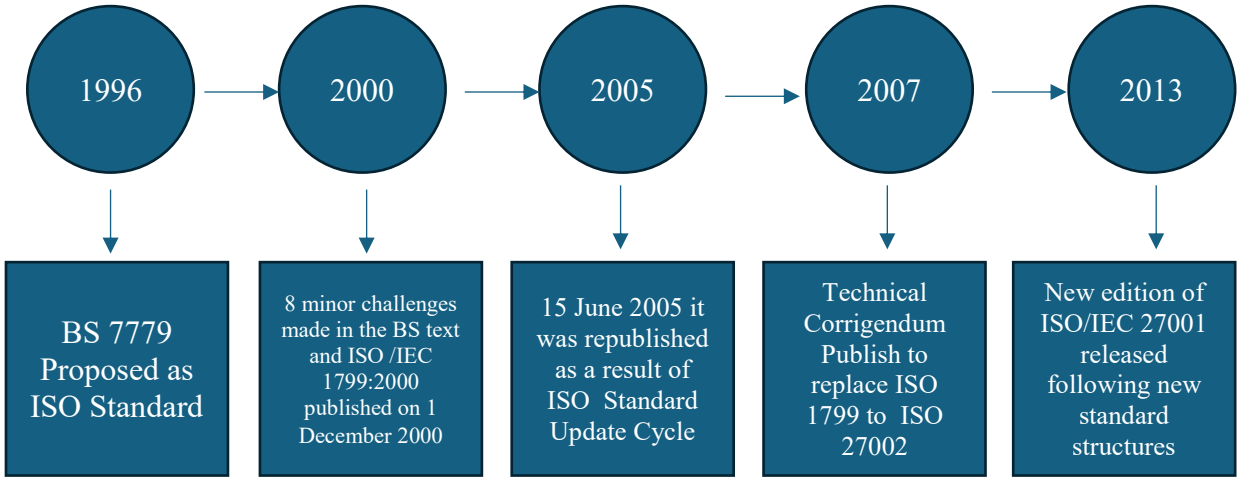
ISO 27001 offers a structured and systematic way to achieve a goal. This standard describes a process for establishing and maintaining an Information Security Management System, which is called ISMS (Beckers, Heisel, Solhaug, & Stølen, 2014). This can be used in any type of organization to secure the information and data that are handled in the organization. An ISMS is a framework of policies and procedures that encompasses physical, legal and technical controls relevant to an organization's information risk management practice. This certification safeguards information against various threats, ensuring business continuity. ISO 27001 was developed to offer a model for establishing, implementing, operating, monitoring, reviewing,

maintaining and improving an information security management system (Kaur, Kochhar, Ganguli, & Rajest, 2021).

3.5.1 Evolution of ISO 27001

Modern Quality Management Standards trace their roots back to the early 1970s. Originating as military standards in the UK, these standards adopted their structure and much of their content from US military standards developed a decade earlier. The US standards incorporated "hard engineering" quality control practices and were influenced by prevailing US management philosophies, particularly "systems thinking" and its application in project management techniques. However, as these standards spread in the UK, some of their original foundations were weakened or altered (Gibbson & Henrikson, 2011).

Figure 1. Chronological evolution of information security standards. Adapted from Kaur, Kochar, Ganguli & Rajesh (2021).



Reflecting upon ISO 27001:2022, information security is a rapidly evolving field. Threats facing the system of information are rapidly growing as business processes are undergoing rapid digitalization. The British Standards Institution (BSI) published BS 7799, a

comprehensive list of information security best practices and regulations, in the middle of the 1990s, which is when the idea for ISO 27001 first emerged (Alrehili & Alhazmi, 2023).

In 1995, the BSI published the BS 7799 part 1, which was guidelines for the establishment and maintenance of an information security management system (ISMS). There had been a BS 7799 part 2 in 1998, which turned the attention towards establishing requirements for the organization's formal requirements regarding the implementation of and certification for ISMS. Such were the standards used to form a blueprint toward the later development of the ISO 27001 (Alrehili & Alhazmi, 2023). Knowing the need for internationally recognized standardization, BSI worked together with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). What resulted from this collaboration was the adoption of BS 7799 Part 2 as ISO IEC 27001:2005, which marked the official presentation of the standard as a global standard for ISMS (Wiander, 2007). BS 7799 Part 1 was simultaneously shoestring to ISO.IEC 17799:2005 is a practical guide for utilizing ISO 27001.

ISO 27001 has undergone several amendments over the years to address the evolving requirement of cyber threats and technology. ISO/IEC 17799 was updated and republished ISO/IEC 27002 in 2007, which contains the latest security controls and best practices. The 2013 versions, ISO/IEC 27001:2013, included newly evolved risks related to cloud computing technologies and technologies with mobile influence (Qusef, A., & Alkilani, H,2022). The latest among these is ISO/IEC 27001: 2022, which greatly enhanced the standard to fulfil today's requirements in the digital environment, with specific emphasis on cloud security, supply chain gaps, and improved interoperability. Hence, by these continuous upgrades, ISO 27001 continues to fly the flag as the leading international standard in information security management across the decades.

With the evolution of information ecosystems driven by technologies such as AI, decentralized platforms, and global data flows, ISO 27001 is likely to face increasing pressure concerning new modalities of risk and governance complexity. The risk-based adaptive framework of ISO 27001 positions it not only as a tool for compliance in the present but also for pre-emption of future regulations in a landscape of fragmented, uncertain privacy (Barafort, 2019; ISO, 2022). As such, future-facing capacity makes ISO 27001 a great aspect for the anticipatory governance of data protection.

3.6 Controls in ISO 27001 and relevance to Privacy

ISO 27001 establishes a detailed framework for organizations. The requirement to establish, implement, maintain and improve an Information Security Management System (ISMS) is ISO 27001. The scope of ISO 27001, therefore, is to bring forth a framework for risk management, leadership, and performance evaluation. ISO 27002 is the actual guideline that explains the details of the best practices and controls for information security management, which particularly complements ISO 27001. Referring to the purposes defined in ISO 27001, the selection, implementation, and management of security controls are dealt with within ISO 27002.

ISO/IEC 27002 is an inseparable component in ISO 27000, being that it is an integral part of the family of standards in ISO 27001. It was derived from the standard ISO/IEC 17799, constituted with acceptable methodology, and renamed to be aligned with the 27000 series in the year 2005. The last amendment of ISO/IEC 27002 was made in 2013. It applies to any size of organization, from micro, small, and medium-scale businesses to large corporations and even non-profit organizations, offering a principles-based approach to the management of information security. The standard is advisory guidelines for the implementation of information security procedures to mitigate risks about the availability, confidentiality, and integrity of information. The 19 sections include asset management, compliance, cryptography, access control, security policies, and physical security.

ISO/IEC 27002, which addresses the controls to be implemented for the firm's implementation of the Information Security Management System (ISMS), is a supplement to ISO 27001. Although they are mostly from the 27000 series, additional pertinent ISO/IEC standards are also mentioned. The interest of ISO/IEC 27001 in management commitment to ensure that these controls are appropriately implemented within organizations serves as a reminder that the implementation of ISO/IEC 27002 controls is crucial from the perspective of the improved effectiveness of the security controls contained in ISO/IEC 27001.

Table 3: Key Differences Between ISO/IEC 27001 and ISO/IEC 27701 in the Context of Privacy Compliance

Aspect	ISO/SEC 27001	ISO.IEC 27002
Type of Standard	Formal specification (mandatory requirements)	Advisory/Guidance standard (recommended practices)
Purpose	Provides requirements for establishing, implementing, and maintaining an ISMS (Information Security Management System)	Provides guidelines and recommendations for implementing information security controls
Focus	Focuses on the requirements for creating an ISMS	Focuses on the implementation of security controls to protect information
Scope	Specifies the requirements for an ISMS applicable to any organization	Addresses a wide range of security controls but does not define an ISMS
Structure	Contains mandatory requirements, including risk management, top management involvement, and continual improvement	Contains best practices for 35 security objectives and 114 security controls
Annexes	Annex A lists controls (from ISO/IEC 27002) to support the implementation of an ISMS	Annex A: detailed controls that can be used for an ISMS, offering specific guidance for implementation
Controls	Defines security controls in Annex A for use in the ISMS	Detailed descriptions and guidance for the implementation of security controls

This table reflects ideas outlined in Monev (2020)

ISO 27001's framework includes seven main components and 114 controls. These components include the Context of the Organization, Leadership and Commitment, Risk Management, Support, Operational Controls, Performance Evaluation, and Improvement (ISO/IEC 27001:2022). These components guide the development and improvement of an Information Security Management System (ISMS) with a strong emphasis on risk-based thinking. According to ISO 27001, controls are countermeasures that reduce security risks through actions like policies or procedures. These controls mitigate threats to confidentiality, integrity, and availability; they are divided into technical controls (cryptography, firewalls), organizational controls (access policies, risk assessments), and physical controls (secure access to facilities) (Peltier, 2016). The controls in Annex A of ISO 27001:2022 aim to support compliance with legal, regulatory, and contractual obligations. They are grouped under the domains that include Access Control, Cryptography, Asset Management, Operations Security, and Incident Management.

Particularly, several controls of ISO/IEC 27001:2022 have direct connections with privacy compliance; most of these also accompany the requirements concerning the General Data Protection Regulation (GDPR). For example, Control A.9.2 (User Access Management) and A.13.2 (Information Transfer) are commonly referred to in cases of enforcement since they focus on strong access restrictions and secure data transfers. According to Suorsa and Helo (2023), failures in implementing these controls have led to costly security breaches. These cases underline the relevance of ISO 27001 controls in operationalizing privacy protections and minimizing regulatory risk.

In a study, Esposito et al. (2022) considered the solid protocol in terms of security and privacy requirements from the viewpoint of the GDPR and international standards of ISO/IEC 27001:2011. The study particularly points out the relevance of control A.18.1.4 (Privacy and Protection of Personally Identifiable Information), which is very useful for ensuring that organizations properly identify and comply with applicable laws and regulations relating to the protection of personal data. The authors find gaps in the Solid protocol's compliance with this control, thus providing ways to improve privacy compliance and enhance the privacy compliance and strengthen its adherence to international data protection standards.

According to ISO/IEC 27001, A.9 (Access Control), A.10 (Cryptography), and A.16 (Information Security Incident Management) are controls protecting personal data. Control A.9 restricts access to information to those who are authorized to view while Control A.10 provides for encryption to protect confidentiality and integrity; and A.16 is concerned with the detection

and management of data breaches in order to limit damage to individuals' privacy in a timely fashion.

The significance of this is to show that data breaches are quickly detected and dealt with problems so as to minimize harm to the privacy of individuals. The effective implementation of these controls strengthens the information security posture of an organization and, at the same time, makes it compliant with privacy regulations, such as the General Data Protection Regulations (GDPR). Organizations will better manage privacy risks by concentrating on these effective controls and demonstrating that they are serious about the protection of personal information.

ISO/IEC 27001 is centred around two fundamental principles that should be followed for effective information security management. These include a risk-based approach and continuous improvement (Barafort, 2019). Clause 6.1 of the standard then requires that organizations identify by appropriate means the information security risks that arise out of their activities and then treat them accordingly in the context of their information security risk management strategy (ISO, 2022, Clause 6.1). Clause 8.2 of the standard states that organizations shall conduct risk assessments for potential information security threats and weaknesses regularly, which requires such regularity so that the security measures applied continue to be valid and effective (ISO, 2022, Clause 8.2). Such evaluations would thus pinpoint areas for improvement and changes to meet new security challenges. Specifically, Clause 8.3 deals with the implementation of the risk treatment plan so that any identified risk is treated. In this study, ISO/IEC 27001 is referred to as ISO 27001 for ease of explanation.

3.7 ISO 27001 and GDPR

ISO 27001 has a major focus on information security in such areas as risk management, data protection by design and accountability (ISO/IEC 27001:2022, Clause 4-10). Therefore, it could be argued that both ISO 27001 and GDPR serve as levers on which to hang technical and operational requirements for reducing breaches. Further, GDPR and ISO 27001 both make sure that a company is resilient enough to take a cyber-attack and an event of an attack, an organization can continue the operations without interruption.

GDPR, on the other hand, focuses specifically on personal data. Not all data is protected under GDPR under Article 4 of the GDPR. Personal data refers to any information relating to an identified or identifiable natural person, which is called a "Data Subject". Information gathered about us is being recorded, processed, and an increasing number of our activities are captured in this manner (e.g., purchasing airline tickets, using credit cards, and using security cameras) (Szabó, 2005, p. 47; Solove, 2004, p. 1).

3.8 CIA Framework

The CIA stands for Confidentiality, Integrity, and Availability. The CIA triad—Confidentiality, Integrity, and Availability—has been a standard way to express security requirements concerning information assets since its introduction in the 1990s (NIST, 2020). It builds the fundamental principles that guide the organization in terms of protecting sensitive data and establishing robust information systems. More commonly CIA is used in standardizing security experts' responses in risk assessments (NIST,2020)

Confidentiality

Confidentiality means sensitive data must be available only to authorized people or entities. Concerning privacy, confidentiality is required so that personal information may reach unintended parties (Anderson, 2008). Data masking and multi-factor authentication (MFA), among others, are strong contenders that maintain confidentiality (Bhargav-Spantzel et al., 2007).

Integrity

The term integrity refers to maintaining data accuracy and consistency throughout its lifecycle. It may be considered an assurance that unauthorized alteration does not modify information. In privacy and security, this can be applied to ensure that personal data is not modified without proper authorization or tracking changes. Methods like hash functions, digital signatures and audit trails are used to maintain data integrity (Shannon, 1949). This concept stands paramount for critical sectors where data must remain consistent and accurate for decision-making.

Availability

Availability ensures that the information and the system are accessible and usable when the authorized users require them. Data must not be rendered inaccessible in privacy and security because of an attack or a system failure. In privacy, availability is important to ensure that individuals can assess their data or that it is available for legal or regulatory purposes. Redundant backup systems and disaster recovery plans are the most common techniques implemented to ensure availability (NIST,2020).

These principles form the foundation of information security and privacy efforts, ensuring that sensitive data is protected from unauthorized access, maintained without alterations and available when needed by those authorized to use it.

3.9 Anticipatory Governance

David H. Guston argues that one needs to understand "anticipation" to comprehend anticipatory governance (Guston, 2010). Anticipation is a word with deep Latin roots. "Ante-", meaning "beforehand," combined with "capere," "to seize or take hold of," brings to bear on the act of mentally "grasping" future possible conditions or events in advance. The anticipation in a contemporary context means developing readiness for probable futures. It is essential in foresight and futures studies and demands proactive planning rather than reacting. By means of this, it does not allow for post-event reactions (Poli, 2017; Miller, 2018).

Anticipation is not merely the ability to predict future events but also involves a proactive engagement with future possibilities, allowing for adaptation and decision-making before events unfold. This means that individuals or organizations can shape their fit through foresight and planning"
(Miller et al.,2015)

Over the past century, different scholars have given different definitions to “Anticipation”. Although there could be differences between the definitions, one definition that could bring the futures perspective. However, even though "Governance" lacks a clear definition, it is a disorganized and ambiguous concept. However, Rhodes (1997) defines governance as the systems, procedures, policies, and practices that govern how a society or organization is run.

To ensure that organizational objectives are met, it entails legal compliance, decision-making, and accountability (Bevir, 2913; Rhodes, 1997).

Within the framework of organizational governance, managers and stakeholders are guided by ethical frameworks and supervision systems that connect the wider interests (Aguilera & Jackson, 2003). Governance is essential for maintaining stability and adapting to change. it provides a framework for setting objectives, mitigating risks and fostering accountability within complex systems (Stocker,1998).

A system of procedures and practices known as anticipatory governance enables communities or organizations to plan and influence future events rather than responding to them after they happen. To manage complicated, unpredictable, and quickly changing situations, it combines strategic planning, adaptive decision-making, and foresight. By using information about possible futures to inform current activities, anticipatory governance promotes resilience and agility in decision-making (Guston, 2010; Miller et al., 2015). It is not solely about predicting future events but also about engaging with future possibilities to make informed, proactive decisions. The concept combines elements of governance, such as decision-making and accountability, with anticipation, emphasizing the strategic ability to envision and prepare for emerging trends and challenges (Poli, 2017; Ramos, 2014).

Memory objects are essential instruments for storing and disseminating foresight knowledge in the context of anticipatory governance, which facilitates proactive decision-making in front of upcoming regulatory issues (Cacciatori, 2008; Ahlqvist). By documenting and disseminating insights across shifting settings, these artefacts enable organizations to maintain consistency and flexibility in compliance procedures (Dufva & Ahlqvist, 2015). Organizations can improve their ability to match forward-thinking strategies with changing legal environments and increase their responsiveness to expected changes in data governance and privacy by organizing foresight into knowledge spaces (Ahlqvist et al., 2012). Anticipatory governance essentially helps form policies and frameworks around which effective responses can be constructed to emergent changes in societal and technological needs through collaboration among a range of stakeholders using tools like scenario planning or futures studies.

3.10 Weak Signals

In Anticipation of emerging privacy frameworks, the researcher argues that weak signals play a crucial role. The history of weak signals goes back to 1970, when Ansoff, who was also a professor, discovered and developed the idea of "weak signals" in Strategic Management (Ansoff,1985). Weak Signals are early and subtle indicators of signs of change that could potentially trigger larger trends. These signals can often be fragmented, ambiguous and hard to detect, yet they have the potential to indicate a significant shift in future. One should anticipate seeing a weak signal. A weak signal can be seen; however, in arguing in favour of the thesis, the researcher finds that to identify a weak signal, one must anticipate a larger consequence of an early detected signal. The uncertain world has actions and reactions, and the reactions to many actions may take a substantially long time to show. Also, in the business world or corporates, where the dynamics are inevitably changing, the weak signals can be seen as an emerging pathway to be better prepared for Future. A *sine qua non* condition, when initiating a new strategy is knowing the relevant environment and anticipating the evolution of the environment, which involves anticipation to trigger the desire to make a strategic decision (Lesca & Lesca, 2014).

In the context of this thesis, the researcher expects that due to the uncertain and fast-changing nature of technology-driven environments, it is necessary to integrate weak signals into the theoretical framework. In such a dynamic environment, innovations happen with greater intensity regularly and there is a greater body of research contributions and policy developments. As technological advancements emerge, weak signals—subtle, early indicators of potential future changes—become critical in anticipating regulatory shifts (Hiltunen, 2010).

With rapid changes in data protection laws, organizations need to develop capabilities for self-gauging early signs of the trends of developing legislation in preparation for compliance before regulatory changes occur. However, the researcher also points out that organizations currently engaged in research, development, and innovation work in Finland need to pay more attention to using weak signals for the navigation of privacy regulations. Privacy is acknowledged as a fundamental right within the EU; hence, organizations conducting research and innovation in Finland need to stay updated with the emerging regulatory trends that may affect their operations in the future (Hiltunen, 2010). Therefore, since most privacy frameworks, including

the General Data Protection Regulation (GDPR) update with the advancement of technology, weak signals help organizations to know in advance the possible changes in legislation, which aid in re-strategizing or adapting their privacy policies early. The researcher expects that, with the integration of weak signals into the theoretical framework, organizations will have the possibility to develop mechanisms for proactive compliance and would also improve their risk mitigation strategies and sustain long-term regulatory alignment in times of quick technological and legislative change.

3.11 Theoretical Relationship Between ISO 27001, Anticipatory Governance, Weak Signals and Privacy Frameworks

This study revolves around the evolution of ISO 27001 with a broader emergence of global privacy regulations as in this context of the thesis is GDPR.CCPA and PIPL. These frameworks have not developed in isolation but rather have emerged as a response to the collective pressures from the technological change, rising public concern over personal data and increasing cybersecurity-related incidents. The perspective of the emergence supports us to see the regulatory shifts not as linear outcomes of deliberate design but as the result of complex and decentralized interaction between legal systems, industry standards and societal values (Miller & Poli, 2010; Holland, 1992). ISO 27001 contributes to this emergent system as a response as well as a co-shaper of global privacy governance, adapting to emerging risks while simultaneously guiding organizations in how to manage them.

In the uncertain future, anticipatory governance complements this view by offering a framework that regulators, industries and standards proactively engage. Digital ecosystems can grow complex and globalized, and the regulatory landscape in response to this development is increasingly difficult to predict. One could argue that the risk-based approach of SO 27001 enhances anticipatory governance by motivating organizations to adopt structured foresight through continuous improvement and risk assessments (ISO, 2022; Barafort, 2019). This proactive strategy supports both the upcoming regulatory developments and the existing privacy requirements. Therefore, anticipatory governance lends credence to the idea that ISO 27001 is not merely a reactive compliance tool but rather a governance mechanism that can impact long-term regulatory harmonization across jurisdictions (Guston, 2010; Poli, 2017).

The foresight dimension is deepened by the integration of weak signals into the theoretical framework of this study. Weak Signals are often ambiguous and early indicators of possible future changes, which serve as precursors to regulatory innovation, technological disruptions or shifts in societal expectations around the privacy of data (Hiltunen, 2010; Ansoff, 1985). Future regulatory reforms, for example, may be influenced by early conversations about algorithmic openness or the security of biometric data. By systematically recognizing and analyzing such signals—for instance, by horizon scanning, policy tracking, or futures analysis—organizations can adapt their ISMS in compliance with ISO 27001 to proactively manage future legal risks. Weak signals thus become operational tools that connect the flexible features of ISO 27001 with new privacy standards.

In ISO 27001, weak signals can be factored into risk management, allowing organizations to anticipate vulnerabilities and change security controls accordingly. This is opposed to a mere reaction after compliance has been enforced. It thus advances the ISO 27001's principle of continuous improvement which risk-based controls ought to evolve with emerging privacy challenges. Further, privacy frameworks like GDPR and PIPL compel organizations to prove their accountability and readiness regarding future regulatory evolution, which strengthens the argument for anticipatory governance/value-based approaches. Embedding weak signal analysis in ISO 27001 risk assessment (Clause 8.2) and anticipatory governance mechanisms also helps organizations to comply better and instill a heightened sense of resilience against future unknowns, while cementing an adaptive privacy management system.

Scenario building in future studies is often carried out according to set chronologies, in tune with anticipatory governance and the examination of weak signals, to allow for the consideration of multiple plausible developments (Miller & Poli, 2010; van Notten et al., 2003). These time horizons are tools for bounding uncertainty and making the future more actionable through present signals. For this study, the shortlist of scenarios is placed within a 5–10-year horizon (2025–2035), which is considered an appropriate timeframe for observing meaningful changes in global privacy governance, the evolution of ISO standards, and the advent of disruptive technologies such as artificial intelligence. Having a defined timeframe allows foresight to be embedded within strategic planning. It so conforms to ISO 27001's philosophy of continuous improvement, which further fortifies the proactive compliance approach underscored throughout this thesis.

A combination of these concepts may present a united approach to put in practice the anticipatory governance and weak signal analysis relative to ensuring that privacy frameworks are put in place appropriately and are maintained. When scenario planning is included with well-defined time horizons, this framework serves to underscore the crucial need for foresight-inspired decision-making decisions to yield data protection stances that are resistant and adaptable.

Chapter 4

4. Data Analysis

This thesis will be conducted through the literature review and the data collection through industry experts. The collected data will be analyzed using the Thematic Analysis by Braun & Clarke (2012). Thematic analysis is about identifying, analyzing, and interpreting patterns of meanings, which are also called "themes" (Clarke and Braun, 2016). The analysis will be done through a process where the data will be divided into themes and codes under the themes. The researcher uses a qualitative data analysis tool "NVivo" provided by the University of Turku to facilitate the coding process. NVivo facilitated the efficient organization of a large volume of qualitative data and helped systematically categorize the themes.

This section presents the key findings derived from the analysis of interview data and provide an in-depth exploration of how these findings address the research questions. While maintaining an analysis of the data from a thematic NVivo coding perspective, this section identifies and organizes key themes based on discussions with industry experts. The themes provide insights on ISO 27001's role in complying with emerging privacy requirements, supporting global compliance with privacy, as well as challenges and benefits related to its implementation. This finds practical features and theoretical understandings to contribute to a larger knowledge scope within privacy and information security management systems.

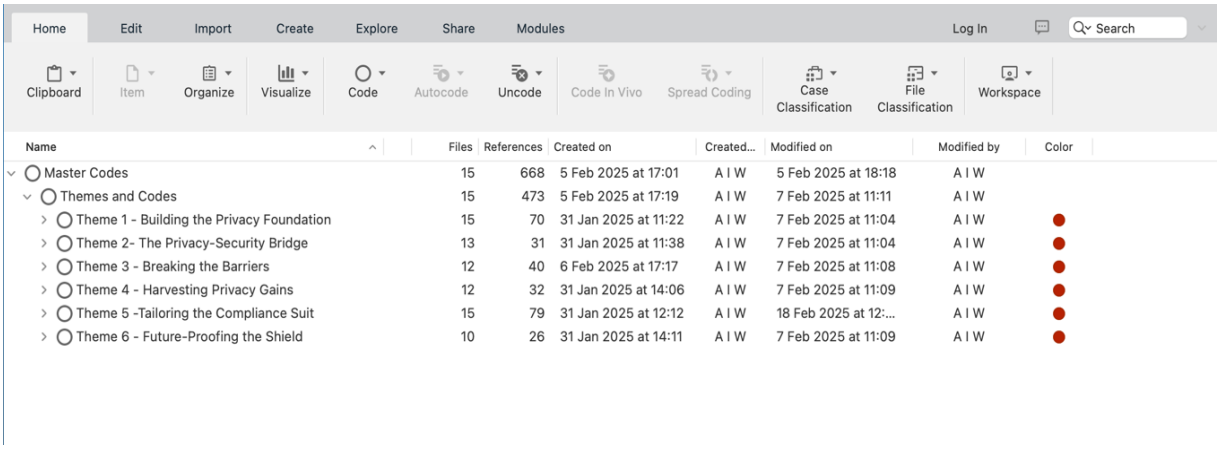
The researcher has collected the data from 15 industry experts in privacy and cybersecurity who are situated in Finland, EU and USA. The methodology makes use of a combination of inductive and deductive coding methods to understand the data. Inductive' coding is a data-driven approach whereby codes, categories, and themes arise naturally from the data without the influence of a conceived framework or theories (Thomas, 2006). 'Deductive coding', on the other hand, is a theory-based analysis whereby the analysis is informed by existing theories themselves, frameworks, or specific research questions (Fereday & Muir-Cochrane, 2006). In this study, deductive coding was used to ensure that key aspects related to the research questions were systematically examined. This maintained the focus of the analysis with respect to answering the research' core objectives' while allowing the emergence of themes through inductive analysis.

In a total of 668 codes were coded and identified throughout the whole data set. These codes were grouped under five themes that directly answer the research questions and relate to the research objectives. The themes captured critically important aspects for organizations implementing ISO 27001 to meet emerging privacy requirements, its contribution towards facilitating global regulatory compliance, and implementation challenges and benefits experienced. A given theme was constructed based on the interconnections among codes, thereby representing both the participants' experience and the theoretical dimension of the research questions. This thematic division makes the complex nature of the local privacy and information security practices across the region with a correspondingly nuanced analysis of the data. The following chapter will discuss extracts from interviews that were categorized under the various themes and codes, providing a better perspective for analyzing the data collected.
To protect the confidentiality and privacy of the interview participants and their organizations, the interview extracts included in this thesis have been carefully edited. Personal identifiers and sensitive organizational details have been modified or anonymized to ensure that no individual or entity can be recognized. These edits were made solely to safeguard confidentiality and do not alter the meaning or integrity of the responses. The content remains faithful to the participants' original insights and accurately reflects the information they provided.

Overview of the Themes

Six themes were generated in relation to the thematic analysis of the interview responses, examining the role, challenges,benefits and future direction of ISO 27001 as it applies in cases of privacy compliance. Each theme consists of codes (subthemes) which were generated based on insights derived from interview participants in the fields of privacy and cybersecurity, specifically directed toward addressing the research questions. The Nvivo theme segregation is shown in Figure 2.

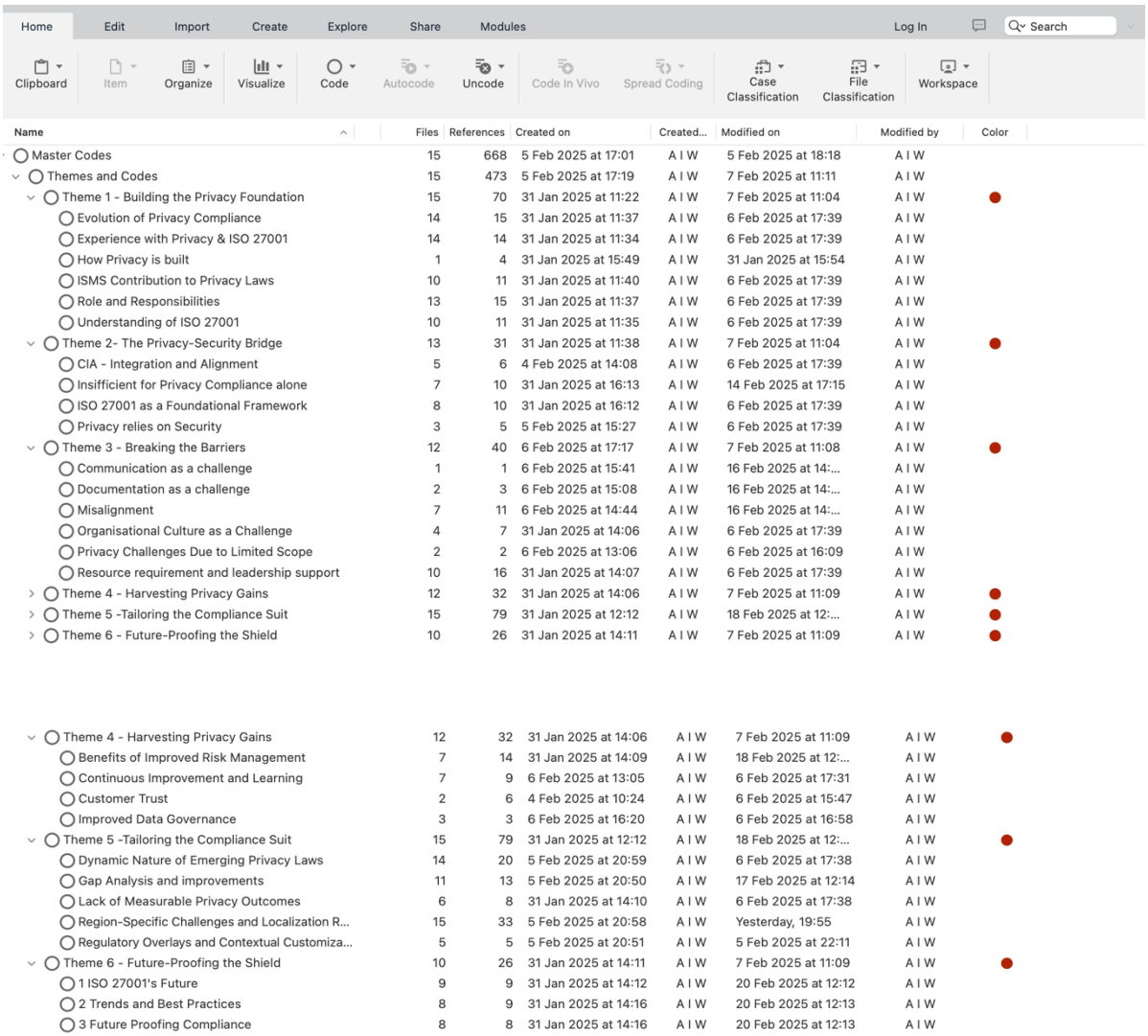
Figure 2. NVivo Screenshot Showing Code Hierarchy



Name	Files	References	Created on	Created...	Modified on	Modified by	Color
Master Codes	15	668	5 Feb 2025 at 17:01	A I W	5 Feb 2025 at 18:18	A I W	
Themes and Codes	15	473	5 Feb 2025 at 17:19	A I W	7 Feb 2025 at 11:11	A I W	
Theme 1 - Building the Privacy Foundation	15	70	31 Jan 2025 at 11:22	A I W	7 Feb 2025 at 11:04	A I W	
Theme 2- The Privacy-Security Bridge	13	31	31 Jan 2025 at 11:38	A I W	7 Feb 2025 at 11:04	A I W	
Theme 3 - Breaking the Barriers	12	40	6 Feb 2025 at 17:17	A I W	7 Feb 2025 at 11:08	A I W	
Theme 4 - Harvesting Privacy Gains	12	32	31 Jan 2025 at 14:06	A I W	7 Feb 2025 at 11:09	A I W	
Theme 5 -Tailoring the Compliance Suit	15	79	31 Jan 2025 at 12:12	A I W	18 Feb 2025 at 12:...	A I W	
Theme 6 - Future-Proofing the Shield	10	26	31 Jan 2025 at 14:11	A I W	7 Feb 2025 at 11:09	A I W	

The main themes had subthemes(codes) under them, and this is reflected in the Nvivo screenshot in Figure 2. Theme 1, Building the Privacy Foundation theme, consisted of 5 codes; Theme 2, The Privacy-Security Bridge, consisted of 4 codes; Theme 3, Breaking the Barriers, Consisted Of 6 codes; Theme 4, Harvesting Privacy Gains, consisted of 4 codes, Theme 5 Tailoring the Compliance Suit consisted of 5 codes and Theme 6 Future Proofing the code consisted of 3 codes. Altogether, the number of references that were subjected to the coding was **668.** Moreover, the number of files was equal to the number of participants, and it was 15. A single extract may fall under different codes due to the complexity and different interpretations of the data.

Figure 3. NVivo Screenshot Showing Main Themes and Subthemes (Codes)



Name	Files	References	Created on	Created...	Modified on	Modified by	Color
Master Codes	15	668	5 Feb 2025 at 17:01	A I W	5 Feb 2025 at 18:18	A I W	
Themes and Codes	15	473	5 Feb 2025 at 17:19	A I W	7 Feb 2025 at 11:11	A I W	
Theme 1 - Building the Privacy Foundation	15	70	31 Jan 2025 at 11:22	A I W	7 Feb 2025 at 11:04	A I W	
Evolution of Privacy Compliance	14	15	31 Jan 2025 at 11:37	A I W	6 Feb 2025 at 17:39	A I W	
Experience with Privacy & ISO 27001	14	14	31 Jan 2025 at 11:34	A I W	6 Feb 2025 at 17:39	A I W	
How Privacy is built	1	4	31 Jan 2025 at 15:49	A I W	31 Jan 2025 at 15:54	A I W	
ISMS Contribution to Privacy Laws	10	11	31 Jan 2025 at 11:40	A I W	6 Feb 2025 at 17:39	A I W	
Role and Responsibilities	13	15	31 Jan 2025 at 11:37	A I W	6 Feb 2025 at 17:39	A I W	
Understanding of ISO 27001	10	11	31 Jan 2025 at 11:35	A I W	6 Feb 2025 at 17:39	A I W	
Theme 2- The Privacy-Security Bridge	13	31	31 Jan 2025 at 11:38	A I W	7 Feb 2025 at 11:04	A I W	
CIA - Integration and Alignment	5	6	4 Feb 2025 at 14:08	A I W	6 Feb 2025 at 17:39	A I W	
Insifficient for Privacy Compliance alone	7	10	31 Jan 2025 at 16:13	A I W	14 Feb 2025 at 17:15	A I W	
ISO 27001 as a Foundational Framework	8	10	31 Jan 2025 at 16:12	A I W	6 Feb 2025 at 17:39	A I W	
Privacy relies on Security	3	5	5 Feb 2025 at 15:27	A I W	6 Feb 2025 at 17:39	A I W	
Theme 3 - Breaking the Barriers	12	40	6 Feb 2025 at 17:17	A I W	7 Feb 2025 at 11:08	A I W	
Communication as a challenge	1	1	6 Feb 2025 at 15:41	A I W	16 Feb 2025 at 14:...	A I W	
Documentation as a challenge	2	3	6 Feb 2025 at 15:08	A I W	16 Feb 2025 at 14:...	A I W	
Misalignment	7	11	6 Feb 2025 at 14:44	A I W	16 Feb 2025 at 14:...	A I W	
Organisational Culture as a Challenge	4	7	31 Jan 2025 at 14:06	A I W	6 Feb 2025 at 17:39	A I W	
Privacy Challenges Due to Limited Scope	2	2	6 Feb 2025 at 13:06	A I W	6 Feb 2025 at 16:09	A I W	
Resource requirement and leadership support	10	16	31 Jan 2025 at 14:07	A I W	6 Feb 2025 at 17:39	A I W	
Theme 4 - Harvesting Privacy Gains	12	32	31 Jan 2025 at 14:06	A I W	7 Feb 2025 at 11:09	A I W	
Theme 5 -Tailoring the Compliance Suit	15	79	31 Jan 2025 at 12:12	A I W	18 Feb 2025 at 12:...	A I W	
Theme 6 - Future-Proofing the Shield	10	26	31 Jan 2025 at 14:11	A I W	7 Feb 2025 at 11:09	A I W	

Theme 4 - Harvesting Privacy Gains	12	32	31 Jan 2025 at 14:06	A I W	7 Feb 2025 at 11:09	A I W	
Benefits of Improved Risk Management	7	14	31 Jan 2025 at 14:09	A I W	18 Feb 2025 at 12:...	A I W	
Continuous Improvement and Learning	7	9	6 Feb 2025 at 13:05	A I W	6 Feb 2025 at 17:31	A I W	
Customer Trust	2	6	4 Feb 2025 at 10:24	A I W	6 Feb 2025 at 15:47	A I W	
Improved Data Governance	3	3	6 Feb 2025 at 16:20	A I W	6 Feb 2025 at 16:58	A I W	
Theme 5 -Tailoring the Compliance Suit	15	79	31 Jan 2025 at 12:12	A I W	18 Feb 2025 at 12:...	A I W	
Dynamic Nature of Emerging Privacy Laws	14	20	5 Feb 2025 at 20:59	A I W	6 Feb 2025 at 17:38	A I W	
Gap Analysis and improvements	11	13	5 Feb 2025 at 20:50	A I W	17 Feb 2025 at 12:14	A I W	
Lack of Measurable Privacy Outcomes	6	8	31 Jan 2025 at 14:10	A I W	6 Feb 2025 at 17:38	A I W	
Region-Specific Challenges and Localization R...	15	33	5 Feb 2025 at 20:58	A I W	Yesterday, 19:55	A I W	
Regulatory Overlays and Contextual Customiza...	5	5	5 Feb 2025 at 20:51	A I W	5 Feb 2025 at 22:11	A I W	
Theme 6 - Future-Proofing the Shield	10	26	31 Jan 2025 at 14:11	A I W	7 Feb 2025 at 11:09	A I W	
1 ISO 27001's Future	9	9	31 Jan 2025 at 14:12	A I W	20 Feb 2025 at 12:12	A I W	
2 Trends and Best Practices	8	9	31 Jan 2025 at 14:16	A I W	20 Feb 2025 at 12:13	A I W	
3 Future Proofing Compliance	8	8	31 Jan 2025 at 14:16	A I W	20 Feb 2025 at 12:13	A I W	

4.1 Theme I – Building the Privacy Foundation

This theme explores the role of experts in and the contribution of ISO 27001 to the emergence of privacy frameworks in their respective organizations. The codes highlight how their respective organizations integrate Privacy into their information security strategies in response to the evolving regulations. The codes under this theme indicate that organizations have adapted their information security frameworks in response to evolving privacy legislation. There are six codes under this theme: Roles and Responsibilities, Experience with Privacy and ISO 27001 and Location, How Privacy is built, ISMS Contribution to Privacy Laws, Evolution of Privacy Compliance and Understanding of Privacy Compliance. Each theme offers insights

and a broad explanation of participants' roles and experiences regarding privacy to build the foundation and basis for achieving the research objectives.

4.1.1 Role and Responsibilities

It is important to get a clear understanding of the interviewee's roles and responsibilities within their respective organizations to ensure quality and relevant output. Prior to the interviews it was understood that these are experts in the fields of privacy and cybersecurity/information security. However, their roles helped the researcher better understand the potential perspectives, which they will continue to do throughout the interview. The perspectives may differ from their own roles and where they are located.

"I have experience in Data Privacy 7 years and overall experience 15 years. Basically, I am as old as GDPR. To get into Data Privacy, I didn't even now this existed before 7 years ago. And when I was working in the company, they decided to have a compliance team, and they gave me responsibilities on the compliance team. I still remember learning the basics in the beginning opening emails and secure emails are different. Now I am working in the financial sector, and I oversee the Data Subject rights that operates in 60 countries." (Participant I)

Participant 1 provides 15 years of expertise and 7 years specifically related to privacy compliance. The participant mentioned that over time, they progressed from learning basic security practices to overseeing data subjects' rights management within the financial institution that is operating in 60 countries; their experience reflects the evolution of the General Data Protection Regulation as well as the relevance of the experience to this study. This background allows them to contribute input from the respective perspectives of fundamental learning as well as high-level cross-border operational responsibilities.

"I work for a multinational corporation as a cybersecurity expert, and it has its headquarters in the USA. I am mostly working with the compliance part of cybersecurity. I make sure that organization's security and privacy programs correspond with global standards and regulations. I supervised the implementation of ISO 27001 to reinforce our ISMS system. I work with the privacy team, so the security controls align with the frameworks." (Participant 9)

Participant 9's input as a cybersecurity compliance expert for a multinational company is critical to understanding how security and privacy are integrated into their daily tasks. This participant has direct experience in implementing ISO 27001 with the privacy teams, which

allows the researcher to understand the strategic importance of the main research question and the subsequent research questions. By gaining insight into the interviewee's role, one may develop practical insights for elucidating how ISO 27001 was implemented as a core security framework and balanced against global industry requirements.

"In my current role, I work with internal audits and consulting, assessing the maturity level of data privacy and information security practices in client organizations and suggesting them improvement actions. In my previous roles, I have worked as a Data Protection Officer for two organizations and as a management consultant. I have also been involved in developing my previous organization's information security management framework in compliance with the ISO 27001 standard."
(Participant 5)

The participant's background in internal audits and consulting allows them to have an extensive awareness of security and privacy procedures. The interviewee's experiences provide insight into the extensive awareness they possess and the practical difficulties they face when implementing ISO 27001 in practice. The interviewee's position in the field of privacy and compliance where the work expeirence provides valuable insight as the participant has contributed directly to ISO 27001 implementation and realises the potential issues that organisations face in doing so. This background offers quality insight to answer the research question of this study.

Similarly other interviewees explained *"I'm privacy officer. I'm responsible for privacy on a group level"* (Participant *9),"* *I'm a consultant on privacy and cyber security"* (Participant 11), *"I serve as a cybersecurity consultant specializing in information security and privacy compliance"* (Participant 12). *"I'm information security officer in a Finnish corporate"* (Participant 13). *"I am a privacy specialist and the appointed Data Protection Officer (DPO) for Germany"* (Participant 14). *"My title was data privacy officer. I lead the global privacy program of the company, and at the same time, I'm the only full-time privacy professionals in the organization"* (Participant 2) which gave a better understanding on which relevant field each of the interviewee has the experience in.

The code "Role and Responsibilities" explains the roles of the interview participants concerning the purpose of ISO 27001 standards, technical assumptions, and implications for privacy and security compliance. Technical knowledge of ISO 27001 varied among participants, and those who had technical or audit-oriented roles demonstrated a deeper

understanding of how security controls play in accord with privacy outcomes. Audits have been recognized by some signatories to be an important element of the standard since they open and create transparency to see what needs to be fixed and improve privacy and security compliance.

4.1.2 Experience with Privacy and ISO 27001 and Location

Geography matters a great deal since the location of the interviewees has a significant impact on their views in terms of privacy compliance and ISO 27001 implementation. Organizations located in areas with strict privacy laws, such as the EU under the GDPR, tend to appreciate privacy frameworks and may tend to see ISO 27001 as a key implementation tool for fulfilling regulatory requirements. On the contrary, respondents coming from countries with sectoral or less comprehensive privacy laws may emphasize other security issues while perhaps taking a different take on privacy integration. The geographic context thus influences their perspectives on the applicability of ISO 27001, the challenges they face, and the level of customization required to respond to jurisdiction-specific legal requirements. Hence, geography is a key consideration in understanding their answer to the research questions.

Participants generally had diversified professional backgrounds in privacy, cybersecurity, and compliance. The experience ranges from a few years to more than three decades. They are all present at different geographical locations across the EU and non-EU spheres, as well as the USA, with some employees attending multinational organizations focused only on compliance and working in multiple jurisdictions. The majority of the participants are found in emerging nations such as Finland and elsewhere in Europe, dealing with privacy and ISO 27001-related matters within their regulatory landscape, particularly under the GDPR. Others operate across the United States and beyond on U.S.-based regulations, specific-compliant sectors, and international privacy laws. A few participants are consultants who cover markets around the globe, which gives them a better picture of the problems and differences in compliance needs according to region.

There was a substantial variation in the levels of experience among participants, some with 20 years of experience in cybersecurity and privacy and others who have transformed their domain in the past five to ten years. Many professionals who have been in the field for many years have witnessed the evolution of privacy laws, including the GDPR and the growing dependence on ISO 27001 implementation, auditing and privacy risk assessments. So, it has added the input

of compliance strategies in their organizations. Some interviewees were new to the field with 3 to 6 years of experience and were engaged in specific privacy-based tasks such as data subject rights management, ISMS audits or adaptation to specific sector compliance requirements. The wide variety of locales and experience levels provides insights into how local privacy legislation influences compliance with ISO 27001 and how the various professionals at different career points view privacy compliance. Further, this input supports understanding the relationship between global and local regulatory schemes shaping the security and privacy strategy of an organization's understanding of ISO 27001.

4.1.3 How Privacy is built

Several participants provided descriptions of how privacy is built up in their organizations, which is attributed to different governance structures, training programs, or compliance mechanisms. The understanding of these structures will allow insights into how privacy is built into the working environments of companies, which is relevant for the implementation of privacy frameworks such as ISO 27001. The scrutiny of these methodologies will help appreciate the development of privacy programs by identifying challenges, strategies, and effectiveness within varied industries.

"We have centralized but distributed privacy management like it would be with any company. If you go to any company in our scale and area of business and range, there should be standalone one. We have a data privacy officer who represents the company in, and that person is from the group of companies. So, there is a central unit, and then we have deeper business in group level. We are centralized, but we are distributed. So, there is a lot of independence on the way we do privacy and infrmation security and we take care of everything with that most diligence, because we can very well say that every single feature that we roll up are compliant, at least in my business group."
(Participant 6)

Participant 6 explains that his organization, in its approach, follows a centralized but distributed privacy management model to ensure compliance within its various business groups whilst independently allowing for implementation flexibility. Governance over privacy is done centrally by the privacy unit led by the DPO (Data Protection Officer), while individual business units independently manage their specific privacy obligations. This hybrid structure allows for a uniform corporate privacy frame, which in turn enables the business groups to implement their privacy practices with respect to their own operational needs.

"We have continuous training, including early trainings for everyone and role-based trainings, all of which are tracked. Our privacy program operates at a high level with both management oversight and technical controls. Many companies do not take privacy as seriously, and during external audits, auditors often learn from our practices. If any gaps are identified, they receive immediate management attention, support, and sponsorship. Overall, my company has a strong privacy culture with a well-established legacy and continuous improvement."
(Participant 9)

Participant 9 explains their approach to privacy governance revolves around continuous improvement and training and awareness programs. Employees receive role-based training and situational training, and they are trained to face incidents using different training tools. It reinforces a good privacy culture. Management oversight and technical controls also play an important role in privacy governance in terms of providing structured mechanisms for monitoring compliance and enforcing compliance. While some participants mentioned the significance of having external audits in evaluating the maturity of privacy practices, such audits tend to reveal that most measures implemented by organizations are beyond audit expectations.

It is important to understand and address the way that privacy is designed and built into the company. Understanding potential privacy gaps proactively ensures minimal compliance risks if immediate attention and support are received from the top management. Such approaches further show how privacy gets infused in various levels of organizations and underscore corporate governance, training, and support since it is critical to have sustainable practices that comply with regulations. Participant 6 explains that his organization, in its approach, follows a centralized but distributed privacy management model to ensure compliance within its various business groups whilst independently allowing for implementation flexibility. Governance over privacy is done centrally by the privacy unit led by the DPO (Data Protection Officer), while individual business units independently manage their specific privacy obligations. This hybrid structure allows for a uniform corporate privacy frame, which in turn enables the business groups to implement their privacy practices with respect to their own operational needs.

4.1.4 ISMS Contribution to Privacy Frameworks

ISMS contribution to Privacy Frameworks code was supported by several interview extracts. It is crucial to find the contribution ISO 27001 as an Information Security Management System

for the privacy frameworks from the perspective of the experts. The relevant extracts and their explanations are as below.

"Even if that is a most modern technique multi factor authentication you have a token in your phone or a device, and when you talk about the encryption algorithm or hashing, these are new things that came in. for example it is very important to check the integrity of data. If you cannot establish the integrity of the personal data that is also a violation of privacy. In the pillar of Privacy there are confidentiality, integrity and availability and these are quite same for ISMS as well. The ISMS is seen as a bigger bucket they go on protecting all types of data whereas privacy is protecting personal data"
(Participant 2)

"ISO 27001 has been significant in evolving privacy frameworks. It is based on the risk-based approach, and it allows organizations to identify and mitigate risks. Even though it doesn't specify what kind of data it ultimately identifies the risks for personal data as well. The continual improvements that are embedded in the standard also ensure that. For example, controls related to data encryption and access management support compliance with the GDPR."
(Participant 4)

From Participant 2 and 4 interview extracts reflects that by establishing security measures along The participants speak of protecting data integrity, confidentiality, and availability through security measures and compliance with privacy. Mechanisms like multi-factor authentication, encryption, and hashing algorithms may certainly be designed to protect data from unauthorized access. Moreover, they bind the data to its rightful accuracy and reliability, paramount for privacy laws, such as GDPR. Further, the interviewees pointed out that data integrity failures could also result in privacy violations. It demonstrates how security and privacy are working together within the ISMS Framework. Furthermore, ISO 27001's risk-based approach, according to Participant 4 above, enables organizations to proactively identify and mitigate tasks associated with personal data before they escalate into compliance failures. This structured approach, along with a continuous improvement process, makes sure organizations remain adaptable to emerging regulatory changes.

"A core component of the ISMS, again, is looking at applicable legislation. So, if you can see where that applicable legislation is applied, then you can connect the ISMS to privacy law. Privacy-related regulations incorporate cybersecurity—again, a core component.

So, regarding how it's affected by other legislation or privacy laws, the way that I approach it is by reviewing those privacy laws, looking at the specific security requirements, and then identifying the gaps in the ISMS.

*It is a core component and a benefit for international compliance. But the key here, as I mentioned earlier, is that it's about **real security**, not just having an ISMS. An ISMS is a management system—it's not a security solution per se."*
(Participant 11)

"Well, I think that, at a high level, ISO 27001 kind of mandates you to identify the relevant regulations and laws. So, in that way, yes, it helps. But it's more like the guidance is coming from the standard that you have to follow relevant regulations—or at least be aware that those regulations exist.
We cannot ignore them. And if we choose not to comply, we have to acknowledge the risk—whether it's due to a lack of resources or some other reason."
(Participant 13)

ISMS functions as a management system rather than a standalone security solution. This means organizations must conduct additional risk assessments. Additionally, interviewees also stressed that ISO 27001 requires organizations to acquire regulatory risks. Still, the effectiveness of such implementations depends on leadership commitment, resource availability, proper security governance, gap analysis, and privacy-specific enhancements to ensure full compliance with laws such as GDPR, CCPA, PIPL, and emerging AI-related regulations. ISO 27001, however, does not provide a *one-fit-for-all solution* to emerging global privacy regulations. Participants stressed that under ISO 27001, organizations identify the applicable privacy regulations and security requirements, so ISMS needs to be compliant with those requirements. However, in their view, ISMS does not intrinsically implement protections for privacy.

"It is not essential for a company to have to have good privacy and security practices. Obviously, it costs money to become certified. It costs money to keep the certification, but it's like me as a privacy professional having a CIPP/E OR CIPM, as a qualification. If I didn't have them, would it mean I'm less knowledgeable about privacy? No, it just a way of showing to again other people, this guy takes privacy seriously. He has a qualification in privacy. There it is. It's an easy way to show that. So that's what I see about having ISO 2700"
(Participant 4)

"I'd say ISO 27,001 sets a higher standard than most privacy laws allow. Again, privacy laws are following one of two pathways. Now, they're all mimicking a GDPR based approach, So, what we're seeing now is obviously ISO 27,001 standards. They've not been officially recognized as being a certification scheme under GDPR, but what it is showing is, is that you're meeting these kinds of standards. The way I see is, if a company has ISO 27,001 certification, they're likely to pass a GDPR audit"
(Participant 8)

In the extracts of Participants 4 and 8, it has been argued whether the ISO 27001 certification guarantees compliance with privacy laws. Participants view ISO 27001 as a prestigious

standard that demonstrates the company's commitment to security. However, it is important to note that having a certification does not necessarily mean an organization is fully compliant with privacy regulations. Similarly, having personal qualifications such as CIPP/E or CIPM (Professional Certifications for Privacy Professionals) also does not mean that the relevant person is more knowledgeable in the area. ISO 27001 sets a high standard, and hence, privacy regulations require additional governance measures such as lawful processing, data subject rights and privacy impact assessments, which are not inherently covered by ISMS.

Nevertheless, Participant 6 noted in the interview that *"companies with strong ISMS frameworks are more likely to pass GDPR and privacy-related audits because it goes hand in hand when proper security controls are in place".* This suggests that ISO 27001 has a significant contribution to privacy compliance. However, it must be complemented with privacy-specific controls, and governance mechanisms must meet the legal requirements as well. Similarly, according to the participants, ISO 27001 is a way to show the outside world that they have acquired the certification, and therefore, a company may have taken information security seriously.

4.1.5 Evolution of Privacy Maturity

Evolution of Privacy Maturity is an important aspect to identify the different stages and the improvements "Personal Data Protection" from the past to today. Privacy Compliance has been evolved significantly during the past years and the importance it was given from every party who deals with personal data is also increased. However, below are the extracts of the experts stating how it has involved in their respective workplaces.

In my personal perspective yes. Of course. We have developed certain matrices to trace how much have this evolved. The programs I have created and how much they have evolved and based on those they have matured considerably. Before 6 years there was nothing and now, we have full blown DSR Privacy teams, privacy incidents, risk assessments, cookies as well as ROPA. If I compare year on year, there is always a gap, and I can say year 2023 to 2024 there is a 10% evolvement.
Participant (10)

"*At least in this company, privacy has evolved a lot. Major steps have been taken over time. After GDPR programs, many companies undertook large projects, but then, for a long period, nothing was done. I believe that many companies are now going back and trying to document everything to maintain privacy. In my company, this process has taken longer, and there has been a lack of documentation work. In B2B companies, many people may not see privacy as as important as it is in B2C companies. However, now people are beginning to understand its*

significance more and more, and awareness of the global aspect has also grown. Especially in Europe, I see that some countries have stricter requirements, particularly the UK and Germany."
(Participant 12)

The extracts of Participants 10 and 12 explain that the evolution of privacy maturity is evident in the structured development of privacy programs within the organization over time. Initially, privacy compliance has been a fragmented concept; however, over the years, it has evolved and has built more structured frameworks around it. These include privacy teams, risk assessments, and incident management, which are all elements of a standard organizational privacy program. Many pointed out that before GDPR, privacy compliance was minimal, if at all. Now, organizations have dedicated privacy functions, technical safeguards and governance structures. Further, Participant 6 described how year-over-year privacy improvements can be quantitatively measured in one of the interviews, bringing the quantitative aspect through the "delta" of privacy engineering.

This high level of privacy focus was embedded into the company's product design process as a part of concepts like privacy by design and default as per the GDPR. Further, another key measure that was highlighted was "continuous improvements" throughout the learning process. Privacy is an evolving field, and with that, companies also should evolve and adapt. However, some companies faced a stagnation period post GDPR where initial privacy projects were completed, but ongoing privacy management documentation took time to mature. Recently, organizations have started revisiting documentation, updating governance structures and reinforcing compliance efforts, demonstrating a commitment to privacy.

Our approach to privacy compliance has evolved significantly. Initially focused on meeting specific regulatory requirements, we have shifted toward proactive and anticipatory compliance. Leveraging frameworks like ISO 27001and the extension of ISO 27701, we now incorporate privacy by design principles, regularly update risk assessments to address emerging threats, and invest in advanced technologies to ensure compliance across our global operations.
(Participant 9)

Participant 9 underlined the evolution of privacy compliance from being a mere regulatory requirement to a strategic approach adopted throughout an organization. Initially, privacy efforts focused more on meeting specific regional compliance obligations such as GDPR.

Organizations are now taking an alternative approach, merging privacy into a more extensive information security framework. This transition demonstrates ISO 27001 as a general framework that companies can apply to meet current regulations. The degree of ISO 27001's application will give flexibility to include new legislation and interpretation in the future, like CCPA and PIPL. Similarly, privacy by design sits within the next set of procedures for development and operation. Hence, the implementation of ISO 27701 essentially aligns privacy best practices with international specifications. Additionally, embedding the Privacy by Design (PbD) principle—an approach that integrates privacy safeguards into systems and processes from the outset—directly into product development and operational workflows is evident in the adoption of ISO 27701 for aligning privacy practices with global standards (Cavoukian, 2011)

"We keep privacy in the most important space. That's why we have these roles to ensure that processes are followed right from the product stage. In my organization, or at least in my company, privacy is everyone's business. That's how I see it at a high level—it's something we communicate, and it's a motto we follow, along with few others. But privacy is everyone's business—that's how we see it."
(Participant 5)

Participant 5 depicts people taking a face to the realities of privacy and seeing it not simply as a compliance issue but rather as an actual business operation. Furthermore, Participant 5 sees that some organizations have adopted a philosophy whereby privacy is deemed a concern of everybody and have cultivated a culture of privacy awareness within all business functions. The embedding of privacy into a corporate process and concentrating the responsibility on everyone have now made organizations realize better than before that they have not only a legal obligation to comply with privacy, but they have established privacy as an organizational value that shapes decision-making and business best practices.

4.1.6 Expert knowledge on Privacy Compliance

At the beginning of the data collection as one of the first questions, the researcher expected the interviewees to have a general understanding of the topic. The researcher carefully selected the industry experts according to their work experience and their involvement in the Privacy and Cyber Security/Information Security community. This theme was developed from the answers of the expert knowledge on personal data protection. However, the researcher ensured that participants represented a diverse perspective with unbiased opinions. So, understanding the

basics approach helped capture well-rounded, unbiased data to build up a flow for the rest of the interview. Below are the relevant extracts and their explanation and relevance to the code.

I know approximately around 93 controls that are important in ISO 27001 and to Privacy. My general observation is the risk or the problem you are finding in privacy has always a solution in security. If someone is unauthorized to access the data and having the access is contradictory. Access Control policy there is a solution for it and that is ISMS. That is my understanding and that is how we keep rubbing shoulders with security guys.
(Participant 1)

"A core component of the ISMS, again, is looking at applicable legislation. So, if you can see where that applicable legislation is applied, then you can connect the ISMS to privacy law. Privacy-related regulations incorporate cybersecurity—again, a core component.

So, regarding how it's affected by other legislation or privacy laws, the way that I approach it is by reviewing those privacy laws, looking at the specific security requirements, and then identifying the gaps in the ISMS.

It is a core component and a benefit for international compliance. But the key here, as I mentioned earlier, is that it's about real security, not just having an ISMS. An ISMS is a management system—it's not a security solution per se."
(Participant 11)

Participants stressed that security measures embedded in ISMS frameworks can mitigate a strong relationship between ISO 27001 and privacy risks. Participant 1 explained that ISO 27001 covers core security principles such as access control, encryption and data integrity. These are also crucial for privacy compliance. However, according to Participant 1. while privacy relies on security, security does not guarantee privacy compliance. It was also noted that ISO 27001 helps organizations align security with legal obligations by requiring them to identify applicable privacy regulations and ensure security controls also meet specific legal standards. These show how ISO 27001 serves as a foundational tool for privacy compliance but does not fully address legal privacy requirements such as data subject rights and lawful processing.

All participants differ in their interpretation and understanding of ISO 27001. In very short terms, they all seem to agree in defining it as a security management system that overlaps with privacy compliance, which is substantial but limited. *"I know 26 controls that are important in ISO 27001 and also to Privacy,"* said one of the participants. *"My general observation is the risk, or the problem you are finding in privacy always has a solution in security. Suppose someone is unauthorized to access the data, and having the access is contradictory. Access*

Control policy: There is a solution for it, and that is ISMS. That is my understanding, and that is how we keep rubbing shoulders with security guys." (Participant 10). Similar arguments are given by some others but pointed out that ISO 27001 remains mainly a technical security framework rather than a standards cover-all for a full privacy compliance system, and hence, different parts of organizations would need to make additional efforts on privacy governance besides ISMS requirements.

An interviewee critically remarks about the controls with respect to privacy in the updated ISO 27001 of 2022: *"I have been pondering on that since in this newest version 2022, there is one new control added which is related to privacy. What is the meaning of that control? Even though that I've heard that it's not taken that seriously when it comes to companies that are driving for the certificate." (Participant 12).* Furthermore, according to another participant, ISO 27001 is said to set a higher standard than most privacy legislation and, conversely, is not officially regarded as certification to fulfil the requirements of GDPR.

"*ISO 27001 is an internationally recognized standard for information security management systems (ISMS). However, ISO 27701 is a PIMS that focuses mainly on privacy. ISMS's relevance to privacy compliance is that it creates a strong baseline for information security risk management that is applicable for confidentiality, integrity, and availability of data. Although it does not set privacy standards, practically many controls connect to privacy requirements such as access controls for data and risk assessment and incident response, so it is a good tool for privacy compliance." (Participant 12).*
Overall, the findings indicate that all participants have an extensive understanding of the ISMS as well as privacy and it was highlighted although ISO 27001 lays an excellent foundation for privacy, further necessary privacy frameworks such as ISO 27701 fill the legal and governance gaps as well providing even an extensive knowledge beyond ISO 27001.

A strong privacy foundation is built upon changing privacy laws and combined with security frameworks like ISO 27001. The results show that although ISO 27001 is essential for security measures that are congruently linked to privacy compliance, it is still insufficient by itself to enable someone to fulfil their legal privacy duties. In addition, organizations must implement continual improvement and privacy-specific governance procedures. As proactive privacy practices were integrated into operations to offset the declining number of regulatory-driven actions, privacy compliance changed. A well-designed ISMS ultimately strengthens privacy

frameworks, but genuine compliance is more comprehensive and includes organizational, technical, and legal aspects.

4.2 Theme II – Privacy Security Bridge

Privacy and Security Bridge represents the relationship between privacy and security. This theme consists of four key aspects, and they are CIA: Integration and alignment, which highlights the need to align Confidentiality, Integrity and Availability (CIA) principles across both domains; ISO 27001 as a foundational Framework recognizing that ISO 27001 serves as a strong base for managing privacy risks but requires additional Privacy specific controls; Privacy relies on Security, emphasizing that privacy cannot be effectively implemented without security controls like encryption, access management and risk-based decision making; and Insufficient for privacy compliance alone, acknowledging that while security framework such as ISO 27001 provides strong data protection, it does not fully address privacy-specific legal and ethical requirements.

4.2.1 CIA: Integration and Alignment

"Even if that is a most modern technique multi factor authentication you have a token in your phone or a device, and when you talk about the encryption algorithm or hashing, these are new things that came in. it is very important to check the integrity of data. If you cannot establish the integrity of the personal data that is also a violation of privacy. In the pillar of Privacy there are confidentiality, integrity and availability and these are quite same for ISMS and PIMS as well. The ISMS is seen as a bigger bucket they go on protecting all types of data whereas privacy is protecting personal data."
(Participant 2)

As explained previously in theme I, under this code, the extract by Participant 2 describes how Privacy and Security are aligned through the CIA triad. The expert highlights that data "integrity" is not only a security requirement but also a privacy necessity. **Article 32 of the GDPR** ties into the aspect of ensuring the security of data processing and the integrity and confidentiality of personal data. Both ISMS (ISO 27001) and the PIMS (ISO 27701) rest on the basic pillars of Confidentiality, Integrity, and Accessibility (CIA), placing farther emphasis on an integrated approach toward security and privacy.

"The key here is that the security controls are interrelated, and what you've got to do with the ISMS is try and make sure that the Accountable people in the organization are using it to steer their security and steer their privacy, but make sure that it's a self-contained and improving

system. So again, continuous improvement is a core component. So, the benefits the discipline of the ISMS is, if you're following the methodology, you have a steering committee, you have continuous improvement, you have risk reviews. So long as they're dealt in the right way and overlaid in the right way, you can use it for privacy. It gets down to accountability, though, so the court of the isms and its use and benefit to privacy is build accountability review and active risk management. So, if you're using it as a tool, and you've built that tool set correctly, then there's a huge benefit with the interplay. If you don't have that tool built correctly, then what you see is privacy do their own thing, or the requirements for privacy within an organization are driven by different people, and there's a divergence from security, rather than a convergence. So again, the interrelationship between the isms and privacy, if you spell correctly, is there is the convergence the ongoing management and the active accountability" (Participant 11)

Participant 11 highlights here the importance of the discipline of ISMS and how having such discipline leads to privacy. This expert also mentions that accountability, risk management and continuous improvement must be embedded in both security and privacy operations. Without this, privacy may operate in silos, and it will lead to a divergence rather than a convergence which weakens the overall data protection strategy.

We talk about confidentiality, integrity and availability. That's the core system and measurement that was set up. And it goes back to the originations of the BS, 575, Now, as I mentioned earlier, regarding AI, you have authenticity and control, which are specific requirements for security going forwards. So, if I consider the limitations again, going to that toolbox, if you are just using 27,001 then every problem is a nail, because you've only got a hammer. If you overlay the 27 701 you've got a hammer and a screwdriver. But again, they have their limitations. The point that I'm getting to is that you have to have additional controls and additional understanding, and you need to modify them to your own context and purpose. If you don't do that, then the benefits of 27,001 isn't met. The benefits of a PIMS aren't met together.
(Participant 11)

Participant 11 highlights the relation of security (ISO 27001) and privacy, considering that CIA needs other specific controls dictated by context. AI and emergent technologies bring into play some extra layers of governance that, apart from classical CIA control, ensure authenticity and control within security. The common analogy stressed is that of hammer and screwdriver to specify: ISO 27001 and Privacy must be enforced together as a full claim for privacy and security perspective.

4.2.2 ISO 27001 as a Foundational Framework

This code represents the extracts that explained where ISO served as a foundational framework. Many participants mentioned that ISO provides a structured security approach that support

privacy and compliance. It was also mentioned that strong security measures such as access control, encryption and risk management does not directly address the privacy specific obligations as week. The extracts below explain the foundational framework in depth.

"That is a good question. Currently I am not seeing that, what am seeing is if someone there are 90 controls. blindly follows the 90 something controls. In 27001 ISMS and 27701 PIMS, I think most of the privacy is covered. The protection part at least. Now what remains is the core privacy, when there is a process for addressing DSR or breach notification, if you already implemented the control the risk of personal data being breached is also minimized, what we have at the moment is sufficient to address these issues."
(Participant 1)

Participant 1 mentioned one of the most critical ISMS and PIMS differences findings. It is important to note that ISMS is an "Information Security Management System", whereas "PIMS" is a Privacy Information Management System. ISO 27001 is an Information Management System, and ISO 27001's extension ISO 27701 is specifically dedicated to building a Privacy Information Management System.It was understood that both ISO 27001 and 27701 provide high-security mechanisms that reduce risks such as data breaches. Yet, privacy is not just protection; it includes compliance elements like data subject request handling and breach notification, requiring governance beyond security. This extract explains why ISO 27001 is a robust base however not a standalone privacy solution.

"ISO 27,001 perhaps, kind of does not kind of respond to any particular feature in privacy laws. I think it's just kind of security standard, and it's, of course, helpful, because there is no privacy without security. But this doesn't go beyond that"

"I think it's helpful in the sense that it gives structure to the security controls, especially, I think, where privacy is handled by the legal department. In such cases, ISO 27001 provides confidence that security is taken seriously"
(Participant 4)

The perspective challenges the assumption that ISO 27001 is a privacy solution. The expert identifies that ISO 27001 directly does not address privacy laws-instead it provides a solid security foundation that enables privacy. Additionally in organizations where legal and security teams operate separately. ISO 27001 provides assurance that security measures are in place. However, the legal team must still implement separate privacy-specific policies to ensure full compliance.

"ISO 27701 is a framework for data privacy that builds on ISO 27001. It guides organizations on policies and procedures that should be in place to comply with GDPR and other privacy regulations and laws. However, these ISO standards are management frameworks, not regulatory frameworks. ISO standards alone are not sufficient to ensure the lawfulness of data privacy practices"
(Participant 5)

Above all, expert 5 distinguishes between standards for ISO, which provide structured guidance but are not laws or regulations. ISO 27001 (along with ISO 27701) provides a structured way to set up privacy measures for the organization. However, Participant 5 speaks of these standards as not exempting any compliance with legal obligations, like GDPR, CCPA, or PIPL. This means that organizations would be expected not only to be ISO compliant but also to integrate mechanisms for compliance with the law and the regulation into their privacy programs.

"ISO 27001 has been instrumental in addressing evolving privacy laws. Its emphasis on continual improvement and risk-based decision-making enables us to adapt quickly to regulatory changes, such as the introduction of the CCPA or China's PIPL. By mapping ISO 27001 controls to specific privacy requirements, we ensure consistency in our compliance efforts globally."
(Participant 9)

Participant 9 shows that ISO 27001's ability to adapt depending on the location or the size. It is a risk-based and continuously improving standard. It is also noted that companies allow to adjust their security and privacy practices as new laws emerge. However, ISO 27001 can be mapped according to privacy requirements which means that it can be applied consistently across globally.

4.2.3 Privacy Relies on Security

The idea that privacy relies on security was noted in several findings of the research and in several extracts. Security provides a safety net to protect the personal data. Encryption, access controls, hashing and pseudonymization and breach prevention are all security measures that directly support privacy compliance. Privacy laws and policies set the rules for how personal data should be handled. However, security is what ensures that if those rules can be enforced in practice. Below is a breakdown of how expert insights highlighted why privacy cannot function without security.

"Even if that is a most modern technique multi factor authentication you have a token in your phone or a device, and when you talk about the encryption algorithm or hashing, these are new things that came in. ex is very important to check the integrity of data. If you cannot establish the integrity of the personal data that is also a violation of privacy. In the pillar of Privacy there are confidentiality, integrity and availability and these are quite same for ISMS as well.. The ISMS is seen as a bigger bucket they go on protecting all types of data whereas privacy is protecting personal data."
(Participant 2)

Participant 2 mentions the core of security measures, which is direct personal data protection. The expert explains data integrity as a prime example: If security mechanisms such as encryption and hashing fail to ensure that data has not been tampered with, then privacy can be compromised. This reinforces that privacy protections are only as strong as the security measures that support them. The reference to ISMS as a "bigger bucket" makes sense since security encompasses all the data while privacy pertains to personal data within its scope in between these two.

"ISO 27001 is predominantly about security, so any security initiative is of utmost importance for privacy. The reason is that privacy as such, privacy controls as such, relies heavily on the security controls. If there is no security, in my view, it's all about false promises. You would say that you have done this. You would have done that, of course then when a security breach happens, all of those promises made becomes false, no guarantee to the rights of individuals who wants those personal data. "Privacy sits on top of security.""
(Participant 6)

This is an extraction from Participant 6, which explains how security supports privacy compliance. Access controls, encryption and breach prevention are crucial for ensuring privacy protection. A company can promise its users that their data is secured; however, if *there is no security, in my view, it's all about false promises"* It is if the security is weak that promises are no longer promises. Further, the expert mentions that *"Privacy sits on top of security."* Reflecting that the protection provided by privacy should be built on security.

"*I don't see that there is a big difference when it comes to security and privacy, except the fact that previously says that. I mean, when you are processing someone's information, there are certain things to follow. You need to the transparency part, and then the contractual aspects, lawful basis and so on. From an actionable point of view, I don't think there should be two separate silos. this should be together."*
(Participant 6)

Participant 6 mentions that security and privacy should not operate in isolation – they need to be aligned. Privacy involves legal aspects as transparency and compliance. However, its

enforcement still depends on security measures. If security and privacy teams work in silos, gaps may emerge, making organizations vulnerable to breaches and compliance risks. When the privacy team and security team work together, it is easier for the organization to embed the organization's policies and processes.

4.2.4 Insufficient for Privacy Compliance Alone

ISO 27001 is a widely recognized security framework, and it is clear from the previous findings. However, under the code “insufficient for privacy compliance alone”, it was categorized the extracts where participants mentioned that privacy goes beyond security and hence, ISO 27001 is not sufficient to fully address the privacy requirements. Below are the key insights and explanations that explain why ISO 27001 alone is not sufficient for privacy compliance.

“We talk about confidentiality, integrity and availability. That's the core system and measurement that was set up. And it goes back to the originations of the BS, 575, oh. Now, as I mentioned earlier, regarding AI, you have authenticity and control, which are specific requirements for security going forwards. So, if I consider the limitations again, going to that toolbox, if you are just using 27,001 then every problem is a nail, because you've only got a hammer. If you overlay the 27 701 you've got a hammer and a screwdriver. But again, they have their limitations. The point that I'm getting to be that you have to have additional controls and additional understanding, and you need to modify them to your own context and purpose.” (Participant 11)

ISO 27001 could be enhanced by incorporating privacy-specific controls, such as guidelines for data subject rights management, consent mechanisms, and data minimization principles. This would make it more aligned with privacy laws and reduce the need for supplementary frameworks.
(Participant 12)

Participant 11’s analogy explains the gap between security and privacy. ISO 27001 is a standard for securing data; however, the expert explains that privacy compliance requires more than just security. Participant 12 explained that governance mechanisms, consent management, data subject rights handling, and even more scope of tasks are needed. Participant 11 explains that simply relying on ISO 27001 for privacy is like trying to fix everything with a single tool in the toolbox. However, ISO 27001 can be even more specific than ISO 27701, which is a Privacy Information Management System and focus. The expert implies that idea: "*If you overlay the 27701 you've got a hammer and a screwdriver”.*

"ISO 27001 has very little to do with privacy. Like I said, it forms the foundations—such as risk management, data leak prevention, and encryption. We discussed dynamic controls, and data leak prevention was there, encryption was there, but it doesn't address privacy directly. It doesn't say, 'Hey, don't collect unnecessary data,' or 'You need to have consent before collecting data.' ISO doesn't say that. It's left up to the company to determine whether such regulations exist in their country."
(Participant 15)

"ISO standards alone are not sufficient to ensure the lawfulness of data privacy practices. GDPR requires the minimization of processed personal data, limitation of retention periods, and transparency in processing. An organization may have reliable information security practices, but if personal data is collected and processed more than necessary for its intended purpose, or retention periods are not defined, or data is not deleted after the retention period ends, or if individuals are not informed about how and why their personal data is being processed and what rights they have, data protection and privacy requirements are not fulfilled. Information security might be well in place regardless."
(Participant 5)

Participant 15 above highlights that ISO 27001 has quite limited involvement in Privacy. In the expert's opinion, they mention that other than risk management and data leak prevention, ISO 27001 does not address the entire need for privacy compliance. According to the GDPR, the principle of Necessity and Proportionality explains that an organization should collect the necessary personal data for its operations. Further, the consent is also an important factor in collecting information in each jurisdictional personal data processing activities. Interviewee 15 mentions that there is no such thing in ISO 27001. In their opinion ISO 27001 has given that freedom for the company to decide depending on their global positioning and the location of the operation. The interviewee 15 and 5 both explain the importance of lawful processing of personal data according to the GDPR as well.

"ISO 27001 is only for managing information security; it doesn't care what the information actually is. It could be business secrets, intellectual property or personal data. ISO 27001 treats all information equally. But personal data is different because it has legal and ethical obligations attached to it. That's why 27001 alone isn't enough-you need to have ISO 27001 or another privacy framework to handle personal data properly."
(Participant 3)

This is an important distinction. The interviewee mentions ISO 27001 treats all data equally from a security perspective; however, privacy regulations/laws do not since personal data protection focuses on "personal data". Personal data requires additional safeguards since it is relevant for regulatory obligations and transparency. Business secrets and personal data are not the same under privacy laws. Their remark also highlighted that relying on ISO 27001 alone

does not guarantee personal data protection. On that note, they also mention that ISO 27701 (Privacy Information Management System), which is the extension to ISO 27001, is a better framework to specifically focus on personal data.

"When I think if ISO, I think of cybersecurity, not privacy, ISO has tried to add privacy elements over the years, but people still confuse security with privacy. Just because you lock data behind a door doesn't mean you' ve addressed privacy. Privacy is about Human Rights, and it is deeper than cyber security. Privacy is about who has the right to access and how they use the personal data, not just about keeping it safe"
(Participant 8)

There are many organizations that believe that if data is secure, then their obligations will be fulfilled with respect to privacy, the interviewee explained. Privacy is more than just the protection of data; it is about who controls data, processes it, and respects people's rights. Interviewee 8 explained that privacy is about protecting human rights, which is one of the core reasons for the existence of personal data protection. Privacy laws require organizations to justify personal data collection, manage consent, and ensure that the controllers/individuals have control over their information, depending on the jurisdiction.

Privacy and security rely on each other, and security is the backbone of personal data protection through encryption, access controls, hashing, pseudonymization, and breach prevention. However, security is not the only factor to consider for privacy compliance, as privacy laws demand proof for data minimization, consent management, transparency, and data subject rights. Interviewees mentioned that ISO 27001 is an excellent framework for securing information; however, by itself, it does not differentiate among the data types and its corresponding legal and ethical duty for upholding personal data. Therefore, it remains insufficient to ensure privacy compliance. According to experts, privacy "sits on top of security," which means that unless secure, privacy protection is meaningless; on the other hand, it does not mean the organizations can simply assume that securing the data means that they are privacy compliant. Privacy does not mean locking away data. Privacy is about who accesses the data, how the data is used, and why it is processed. Since ISO 27001 was created for general information security rather than specific privacy-related requirements, organizations should use it in combination with relevant legal frameworks and align operational activities. Ultimately, the extracts highlight that privacy and security must work together to build a truly compliant and effective data protection strategy.

4.3 Theme III - Breaking the Barriers

The theme Breaking the Barriers emphasizes the challenges that organizations may face when implementing ISO 27001 in the context of privacy and compliance. ISO 27001 provides a solid basis for information security, but its implementation faces challenges such as communication barriers, documentation upsurge, leadership support, culture in the organization, and how such culture influences the addressing of privacy needs under the ISO 27001 requirement. The following are the various codes placed under the breaking the barriers theme, with references and comments from interviewees pertinent to the codes.

4.3.1 Resource Requirement and Leadership Support

Resource requirements and leadership support codes represent the data that was collected from the interviewees, who emphasized the importance of resources and leadership in implementing ISO 27001 in a corporate context. Relevant extracts that support this code and the explanations are as follows.

"*The most critical is the management who approves the budget. If there is no budget nothing happens. Then the human resource to take the project up. Sourcing the talent is also another thing. So, if you take care of these then the employees are the very critical part. They are also the key that security is intact, and they are also the weakest link, and breach can happen at any time."*
(Participant 1)

The participant states that funding and allocation of the resources is the primary challenge in implementing ISO 27001. The expert further mentions that organizations do not invest in security infrastructure, privacy tools, and skilled personnel without approval from management. Additionally, it is difficult in finding qualified professionals with an expertise in ISO 27001. Employees are essential to security and possible vulnerabilities, as continuous investment in training and awareness is required.

"Top Leadership! Definitely. They must support this. This is a big exercise, and they must be like spokespersons for the work all the time, supporting it heavily. But then, of course security people, IT people, privacy people, HR, Physical Security as a whole, I believe. " (Participant 10)

"If you don't have the right level of sponsorship and the right level of understanding of the benefits and the need, then it gets very difficult, and very often I see an isms being implemented as a sales need, rather than a perceived full organizational need. And then beyond that, there's

the burden of control. So, I have one organization that I work with, and I'm constantly chasing them to make sure that they're managing their risks, they don't like managing their risks. So, it's continual learning process. Getting the right implementation to the right requirements involving the right people and ensuring continued commitment is key"
(Participant 11)

Above both participant 10 and 11 expresses that importance of the leadership as well as sponsorship. The cross-functional collaboration from Security, IT, and Human Resources is also recognized as an important aspect of implementing ISO 27001/ In many cases, organizations pursue ISO 27001 for external compliance reasons such as sales, buyer requests or certification needs rather than genuine integration to their security and privacy culture. Participant 11's input mentions that it creates a superficial approach where companies fail to manage risks effectively. The experts also mentioned that without continued leadership commitment and ongoing training, ISO 27001 remains ineffective.

"Critical resources include skilled personnel with expertise in both ISO 27001 and privacy laws, robust IT infrastructure for implementing technical controls, and strong leadership support to prioritize privacy compliance."
(Participant 12)

"You need to have the support of senior management, which in Finland means board of directors and CEO, If they do not fully back you, you cannot do this. This is not a CIO project, and CIO cannot do this otherwise."
(Participant 3)

Participant 12 proves the main critical points that were previously stated by Participants 1,11, and 10 about resource allocations and leadership support. Participant 3 further mentions the importance of executive buy-in, especially in hierarchical organizations where board-level decisions dictate priorities. In many cases, ISO 27001 is forced down the IT or security teams, but in the absence of high-level support for budget, personnel, and whole organization commitment, its effective implementation becomes almost impossible. Hence, privacy and security efforts cannot go ahead without the support of the board and cannot solely be the responsibility of the IT teams.

"It's more a case of hiring the right people in the right place. It's having a privacy team in place, whether it's one individual acting as the sole privacy representative. Or whether it's having a team of 20 or 30, it's, you know, again, it depends on organizational size. It's having a security team in place, whether that is working from a more security assurance perspective, or whether that's working from an instant response perspective. It's setting the foundations that privacy and security are features that are taken seriously within that so those are the resources that you need."

(Participant 4)

"One of my major challenges was getting an internal auditor to audit its compliance status against the ISO standard. We had a small team and no internal auditor, So, we had to hire externally which was very difficult. Another challenge was benching off what would be acceptable for the final audit. Management buy-in was key, otherwise, you don't go anywhere. Collaboration between several teams was also a challenge since privacy and security require input across operational, technology, and legal."
(Participant 7)

Also, Participant 4 emphasizes the need for structuring privacy and security teams. Smaller organizations may not have dedicated privacy professionals, which forces one person entirely to do all the privacy compliance, while larger companies require a set of teams to work on security, privacy, incident response, etc. However, it has been really emphasized that expertise makes the difference when it comes to the effective implementation of ISO 27001. Participant 7 brings a personal experience of difficulty, saying that they found it difficult to find an internal auditor, thus emphasizing the importance of hiring the right people for the right tasks.

4.3.2 Misalignment

A common challenge organizations face is the lack of harmony between ISO 27001 and the compliance with privacy regulations. The ever-ambulating nature of privacy is, of course, much beyond the dimension of security-privacy requirements that center on the data subject's rights, legal obligations and the jurisdictional differences. Many companies struggle with aligning security and privacy frameworks, integrating multiple standards, and ensuring compliance across different legal landscapes. Here are some of the most relevant extracts with meanings within the challenge.

"We have global legislation, but it's difficult to take all of it into account—or even know what exists around the world. So, I don't really know how that can be done. It's very challenging. Most likely, it ends up being the same as always: we just refer to the most well-known regulations that fall within the scope of the certification. Then the company briefly reviews those. For example, in China, I know there are stricter rules regarding personal data."
(Participant 10)

"Challenges include aligning the ISMS with specific privacy requirements, managing cross-border data transfers, and ensuring employee awareness of privacy obligations. Additionally, integrating ISO 27001 with multiple privacy frameworks can be resource intensive."
(Participant 12)

Organizations across the world face challenges aligning ISO 27001 with privacy requirements in view of the different legal frameworks in different jurisdictions. Participant 10 captures the essence of the complication of compliance with many privacy regulations; trade-offs have to be made so that the more familiar ones-GDPR-are prioritized over others with which companies are less acquainted, perhaps even stricter national rules like China's data localization, which is mentioned in the PIPL. Compounding factors involve variations in the regulations' very definitions of important terms like sensitive personal data. Similarly, Participant 12 emphasizes that aligning an ISMS with privacy frameworks is complex and resource-consuming in terms of integrating multiple frameworks while cross-border data transfer compliance and employee awareness of privacy obligations. The above challenges further illustrate a mismatch: ISO 27001 is engineered from the perspective of security, whereas privacy compliance entails a somewhat wider, regulatory-specific view that requires the adoption of alternate frameworks and customized approaches to adequately compensate for the mismatch.

"The upshot is that they've got certified because an auditor, and this is the biggest problem with this standard, and many other standards, is an auditor just wants to see a control and some evidence to see that it's been implemented. They're not measuring the efficacy of the control, and they're not measuring the appropriateness to the organization. So the key here is that with regard to the specific standards, you need skilled people who understand how to implement to bring the best benefit from the standard to deliver security and to deliver a meaningful service to the organization based around security and privacy, which meet customer requirements, which meet the requirements of the standard and meet the business need for enhanced security and privacy."
(Participant 11)

Participant 11 explains a fundamental misalignment in the application of ISO 27001. The main concern is that organizations treat certification as a checklist exercise instead of integrating it into meaningful privacy protection. Participant 11 stresses that the problem lies in the auditors not focusing on the actual privacy and security implementations but rather looking for documentation and evidence. In some cases, this results in a false sense of compliance, where the companies appear to satisfy the requirements of ISO 27001 on paper while being noncompliant with real-world privacy tasks.

"ISO 27001 is only for managing information security; it doesn't care what the information is. It could be business secrets, intellectual property or personal data. ISO 27001 treats all information equally. But personal data is different because it has legal and ethical obligations

attached to it. That's why 27001 alone isn't enough-you need to have ISO 27001 or another privacy framework to handle personal data properly."
(Participant 3)

The above extract of Participant 3 highlights a structural misalignment where ISO 27001 treats all data the same. Privacy regulations often distinguish personal data from other data types. ISO 27001 does not limit its focus to the type of data. Further, ISO 27001 has guidelines that are in accordance with ethical and legal obligations; however, companies need to implement what is suitable for their requirements. The participant suggests ISO 27701, which is a privacy information management system, would be better suited to tailor the privacy requirements.

4.3.3 Organizational Culture as a Challenge

For the successful implementation of ISO 27001 and privacy compliance, organizational culture is crucial. A poor security and privacy culture could result in the employees disregarding data protection, leading to issues in compliance, security breaches, and a lack of commitment to privacy best practices. The following extracts are taken from interview transcripts under the code of organizational culture as a challenge to explain why experts saw culture as an important element in implementing a privacy-focused Information Security Management System.

"The biggest challenge is the culture part. Everybody has to think that this is important security and privacy is important. Whether you are dealing with data or not data the whole org has to think in one direction. I am responsible for protecting my own computer and my own data. That culture is tough and it cannot come in one or two years. there will always be incidents when someone has accidents. Not blaming humans but if we give up on a proper company culture the next incident happens too fast. The biggest challenge I think is the Culture."

"You must also have the sense of culture. When I say culture or compliance, doing the right thing even when nobody is watching me. That sense of belonging should be there. These are the necessary things that I believe is critical."
(Participant 1)

Participant 1 mentions the importance of culture on separate occasions in the interview transcript. According to them, culture is one of the fundamental challenges in implementing ISO 27001. Building a strong security and privacy culture across an organization is not an easy task. Implementing security controls to comply with regulations is not necessarily sufficient. Participant 1 emphasizes that employees at every level should have the "privacy mindset" and "*do the right thing when nobody is watching me".*

“ISO 27,001 it's the adoption of, building your management system, or if you have the management system in place. But then how to do the actual implementation and adoption and throughout the organization in which it's relevant, like policies, would be relevant pretty much to the older employees. Otherwise, What's the sense of information security, management System? if everybody who is handling their corporate information do not identify that, hey, they would need to maybe protect in somehow be aware that they need to develop their skills. They have to do some mental retraining.”
(Participant 13)

According to Participant 13, policy alone is not sufficient; organizations must also ensure that employees understand and apply those security and privacy principles to the course of their work. Awareness and training programs should be a part of the learning process of day-to-day activities rather than one-time events to keep employees more engaged and informed. The challenge here is that employees tend to view security and privacy as the prerogative of IT rather than their own, resulting in disinterest and inconsistent measures taken toward the security of systems. That needs to be addressed to tackle the issues.

"It’s about showing a healthy respect and need for security and privacy. Resources are critical—whether it’s hiring the right people, building a privacy team, or ensuring that security is taken seriously. The organizational culture must reflect that security and privacy are essential, not just compliance checkboxes."
(Participant 4)

In this context, Participant 4 explains that the culture within an organization is the one that really decides whether security and privacy are genuinely regarded or just seen as a matter of compliance. Most companies see achieving ISO 27001 merely as a goal for certification, and that produces only minimal effort on their part beyond whatever is required for audits. When there are no leadership initiatives or investments in the privacy and security culture, compliance might be very much on the surface, reducing the chances of compliance and increasing the effectiveness of security vulnerabilities.

4.3.4 Documentation as a Challenge

Several Participants highlighted the documentation as a challenge in the process of ISO implementation and aligning it with privacy requirements. Below are the extracts and the explanations that showcase the documentation challenge.

"What am seeing is if someone there are 90 controls. blindly follows the 90 something controls. In 27001 ISMS and 27701 PIMS, I think most of the privacy is covered. The protection part at least. Now what remains is the core privacy, when there is a process for addressing DSR or breach notification, if you already implemented the control the risk of personal data being breached is also minimized, what we have at the moment is sufficient to address these issues." (Participant 1)

Participant 1 remarked that both ISO 27001 (ISMS) and 27701 (PIMS) cover most aspects of security, though documentation remains one significant gap in relation to privacy-specific requirements like Data Subject Rights as well as breach notifications. Following ISO 27001 reduces individual data breach risk while requiring organizations to have clearly documented processes to prove their compliance. This means that even if technical security measures are in place, privacy obligations require additional documentation. Participant 1 states that this is something that companies struggle with. Proper documentation is required for companies to address the privacy requests or security breaches even with a strong security.

"Providing documentation. So, when the assessor comes in, they will require set pieces of documentation. Now, a lot of the time with other businesses, it may be documents that they don't necessarily have, or it may be documents that they need to hastily write up. So, these, these are the issues is on. You'll have one system set up like, like I mentioned earlier, this meeting recording on your personal device. Device, put it on a hard drive, wipe your personal device, clean it on a portable hard drive. Put them in a safe. Put that in a safe outside. Out of Mind. You and I both know that's going to meet an ISO standard because it's kept in a secure environment, limited access control, and you know it can't be copied or excavated or transferred."
(Participant 4)

This expert also states how intensively the documentation process is handled in the ISO certification process. Participant 4 mentions that some companies or businesses struggle to produce the required records when an auditor comes in. Some companies do meet the ISO standards in practice; however, due to the lack of necessary documentation, they fail the compliance assessments. This shows that even if an organization follows proper security measures if they cannot prove it through detailed records, it might not count towards the audit. Additionally, some companies may only realize the importance of this when they go through the process due to time and resource constraints.

"When an ISO 27001 auditor comes in, you need to have documentation showing that you've done everything required. You need written evidence, all logged — what you've done and when you've done it. That's the difficulty: a lot of companies already meet the standards, but they

don't have the evidence, and many don't even realize they're compliant. They focus on the cost of getting certified and think, 'We don't have the time or resources to commit to that right now.'

Another issue is that you don't know what kind of assessor you're getting. One assessor might come in with a very different standard than the next. Their thresholds for what counts as a pass or fail can vary significantly. For example, in one instance, an auditor was happy just talking to me. They came in, asked about my two-year plan — what standards I aimed to achieve — not necessarily what I had already produced. They were satisfied with those answers.

But with a different assessor, that wouldn't have been enough. They would have asked, 'What have you delivered? Where's the documentation? Where's the proof?' Some are okay if you say you're going to do something and have it clearly planned — they'll say, 'We'll come back in two years.' But that kind of variability between auditors can be a real challenge."
(Participant 4)

The above extract is a significant finding where the interviewer explains in a "role play" of a hypothetical situation. Participant 4 explains here that another challenge that companies face related to documentation is that different assessors may have different interpretations of what is required for compliance. Some auditors may be lenient-auditors who may accept future and verbal commitments-while others strictly require proof of implementation through documentation. This inconsistency may create an uncertain environment for organizations as they may not know whether their documentation efforts meet the expectations of the auditor. The participant explained that companies that had invested heavily in documentation might have found themselves with another auditor who would not have required that much documentation at all. Thus making it a tedious and unpredictable part of compliance.

Documentation challenges within ISO 27001 compliance are more than just paperwork. It is about the systematic understanding and clarity of evidence that the organizations have provided for their security and privacy practices. Many companies are compliant with security requirements but fail to document their processes adequately, thus making it difficult to demonstrate compliance. Auditor inconsistency adds to the dilemma as organizations cannot always predict what level of documentation is required; hence, businesses must work to establish regular document storage so that they are prepared for any audit scenario that may come across.

4.3.5 Privacy Challenges due to Limited Scope

Participants highlighted the scoping limitation as one of the barriers to align the different privacy frameworks to ISO 27001. Following are the extracts of interviewees explaining why the limited scope is a challenge in privacy compliance in line with ISO 27001.

"It's easy to show a paper saying, 'We are ISO accredited.' If you don't believe us, go ask ISO. Instead of saying, 'We take privacy and security seriously—here's this stack of documents that proves it,' which could be a lie, or an attempt to trick you, or just a bunch of documents generated by ChatGPT, having the actual ISO certificate says: 'Don't believe us. Believe this accredited organization.'

Their entire credibility—and essentially their whole business—rests on being trustworthy, on providing that standard, that voice of reason."
(Participant 4)

Participant 4 indicates one of the important key points in ISO certification, that is perceived compliance versus real privacy actions. The interviewee states that the companies can treat it as a seal of approval for many organizations rather than really embedding privacy and security into their daily practices. While ISO 27001 may provide some credence, it does not automatically mean that the organization is actively upholding strong privacy and security protections. Therefore, companies treat ISO accreditation as an external validation or even as a checkbox exercise without genuinely implementing strong privacy measures. In such a case, there will be a gap in compliance and real-world privacy protection, where companies look compliant on paper but might not be fully committed in practice.

"I think the part where people often get tripped up with ISO is that it's a very robust framework—but not all companies do all the things it outlines. So, the challenge becomes figuring out what applies to them and what doesn't.

Some companies might think, 'Okay, this is on the list—we don't do this, but maybe we should, or maybe we should claim that we do.'

I think the challenge with almost any framework is for companies to clearly state what they do and what they don't do, without wasting time trying to create the impression that they're doing something they actually aren't."
(Participant 8)

"A company in Finland may have ISO 27001 certified and also small textile company in rural India may also have the ISO 27001 certification. This does not mean they have the same level

of security in place. The level that each company needs to adhere may be different. This can happen in different industries or even within a one company in different sub sections" (Participant 10)

Participant 8 states that even if ISO 27001 accreditation is in place, its effect varies depending on the implementation. Some companies struggle with understanding what should be included and what is irrelevant to their operations. Some companies tend to over-associate documentation with controls that are not in line with the company's operations, while some do not consider some aspects of privacy because they don't specifically mention anything related to such aspects under ISO 27001. This creates inconsistencies in the application. Some companies find resources wasted trying to figure out the most relevant criteria or don't try to address the gaps because they believe the compliance level may have been enough. Further, Participant 8 explained that different levels of security controls could be needed depending on the level of security determined. It can vary from industry to industry, country to country or even between different sub-parts within the same company. Participants highlighted the scoping limitation as one of the barriers to aligning the different privacy frameworks to ISO 27001. ISO 27001 is a costly process for any company, and it is quite important to understand if a company is large in geographical size or human resource size, to which scope the implementation of ISO 27001 should be applied. Companies must strategically apply the certification to the areas where information security is needed the most. Following are the extracts of interviewees explaining why the limited scope is a challenge in privacy compliance in line with ISO 27001.

4.3.6 Communication as a Challenge

Several Participants stressed the challenges related to communication during the process of ISO 27001 and privacy related requirements. A multinational company can have employees from different backgrounds whose study level and experience are vary. Several extracts explaining this barrier are explained in detail below.

"There's often a communication gap between the different roles involved in these activities. Sometimes, people coming from a legal background have no clue about the technology. And then there are highly technical people—some are deeply immersed in backend systems, black screens, and very niche technical issues.

So, when we talk to them, there's a clear mismatch in communication styles and approaches. A person with a purely legal background communicates very differently from someone with a purely technical background. The level of detail, the terminology—they often just don't connect well.

I would say that, because of the diversity of roles involved, establishing or maintaining effective communication—or developing a good communication equilibrium—is actually a real challenge."
(Participant 6)

Participant 6 states, one of the main challenges is the communication challenge in all aspects of implementing ISO 27001 for privacy compliance. There is a gap between legal professionals and technical professionals because the terminologies used by one in their day-to-day work and in their education may be borrowed from different fields. Lack of communication between the field professionals during implementation is common. The legal professionals may not understand technical aspects, and vice versa. A common understanding of the identification of key privacy risks should exist. In addition, some technical experts engage very much in back-end development and cybersecurity operations in very complicated environments, which could be hard for legal teams to follow. Without this common language and methodology for structured communication, makes it hard to close the gap between secure privacy efforts and compliance. Cross-disciplinary training has to be provided to generate lucid documentation for both legal and technical teams while creating channels for structured communication.

There are many challenges an organization encounters while implementing ISO 27001 into practice for privacy compliance. Communication gaps between the legal and technical fields, a large number of documents which standards must be upgraded, inconsistencies between information security and privacy regulations, organizational culture limitations, and top management support and availability of resources with the limited scope of ISO 27001 concerning privacy completing the list.

Without a proper communication channel between the technical and legal departments, the difference in perspectives may later be innefctive to privacy compliance. Demonstrating compliance became harder due to the amount of paperwork to go through, even when a company had, in fact, complied with the security stipulations in practice. The incompatibility between ISO 27001 and privacy laws makes it difficult to properly adjust the framework to national laws and frequently results in gaps in compliance. Culture is critical here; if employees lack a strong consideration for security and privacy, ISO 27001 becomes only a compliance

exercise. Obtaining funds, staff, and implementation experience are always dashed due to a lack of resources and support from leadership. Finally, the narrow scope of ISO 27001 regarding privacy compliance means the organization will be compelled to scour for other frameworks, perhaps ISO 27701 or ones from the region, that will help it comprehensively cover its obligations toward privacy.

To address these challenges, organizations need to conduct continuous training, foster cross-functional cooperation, obtain full leadership approval and include pertinent privacy-enhanced software frameworks in their own information security management systems. The unjustified denial could turn ISO 27001 into a compliance instrument rather than a comprehensive framework for security and privacy governance. Organizations would be able to create a privacy-sensitive security management framework that supports risk management and data protection policies and guarantees compliance if these obstacles were removed.

4.4 Theme IV- Harvesting Privacy Gains

There are four codes under the theme "Harvesting Privacy Gains". The codes that shall be discussed under the theme are Improved Risk Management, Improved Data Governance, Continuous Improvement and Learning and Customer Trust. Harvesting gains consist of the positives and the benefits of ISO 27001 to Privacy Compliance that participants expressed during the interviews. The mentioned benefits have been coded under the mentioned codes. The detailed extractions and explanations of the codes under "Harvesting Privacy Gains" follow.

4.4.1 Improved Risk Management

One of the main benefits that interviewees repetitively mentioned was the improved risk management. And how the risk-based approach of ISO 27001 minimizes the risks related to personal data as well as data. Following are the extracts that participants have mentioned during the interview on improved risk management.

"Now what remains is the core privacy, when there is a process for addressing DSR or breach notification, if you already implemented the control the risk of personal data being breached is also minimized, what we have at the moment is sufficient to address these issues."

"The personal data breaches have significantly subdued over the time. The moment we decided to have a MFA in our organization a role-based access control, the moment we be serious about the classification of information and apply the pseudonymization and anonymization, the incidents have reduced."
(Participant 1)

Participant 1 states that implementing controls under ISO 27001 and 27701 reduces privacy risks regarding Data Subject Rights and breach notification. Participant 1 emphasizes a structured approach to risk management to help end up with fewer breaches of personal data and better privacy compliance as an outcome. The expert also mentions that personal data breaches have significantly subdued over time, and the impact of risk management strategies such as Multi-Factor Authentication (MFA), role-based access control and data anonymization has been along the implementation of ISO 27001. These measures have increased security and reduced the frequency of incidents related to personal data breaches, which demonstrates how privacy risk management improves through ISO 27001.

"ISO 27001 has been instrumental in addressing evolving privacy laws. Its risk-based approach allows organizations to identify and mitigate risks related to personal data, while its emphasis on continual improvement ensures readiness for new regulatory requirements. For instance, controls related to data encryption and access management directly support compliance with GDPR and PIPL."

"ISO 27001 could be enhanced by incorporating privacy-specific controls, such as guidelines for data subject rights management, consent mechanisms, and data minimization principles. This would make it more aligned with privacy laws and reduce the need for supplementary frameworks."
(Participant 12)

Participant 12 explains how ISO 27001 has been addressing the evolving privacy laws and emphasizes the risk-based approach, which allows companies to mitigate the potential risks related to personal data. The emphasis on continual improvement and the specific controls related to data encryption and access management directly support minimising the risks related to privacy compliance. Further, the interviewee suggests ISO 27001 can be enhanced by adding privacy-specific controls for guidelines for data subject rights, consent mechanisms and data minimization.

"There are good controls that you can use, and if you identify privacy related risks, you can apply for controls to mitigate the risks."

"It should help us identify the risks related to personal data. At least, that's one of the approaches that we have taken that. In our ISMS that we want different units, different functions to identify the different kind of assets, including information assets that they need to protect or what information has value to them, or what information, if the information would leak out from the organization, what would be the cost to us, and then leading To the risk management that when you have the assets identified, then you start, then you can start estimating the risks, what can be relevant to each asset."
(Participant 12)

The Risk Management certainly is a kind of benefit for privacy compliance, and also many of the security controls implemented in the organization and training, security related training certainly is, is a benefit for privacy compliance. And also, I think in practice, it has prevented many, many privacy bridges. Kind of improved security posture of the organization.
(Participant 2)

"I would say. It's improved our risk management. Now we have a risk management matrix that is more aligned with global standards. Before we got the certification, we did not have that. So I will say it has really, really helped our privacy compliance in a lot of ways also, yeah, relating to data governance as well. It has also been very, very helpful, because, again, we have a labelling system that can also be benchmarked against the global standards as well. And beyond that, it's also easier for us to be able to like, patch through security certifications. Maybe we are contracting with an organization, we can easily say, Oh, we have the ISO certification, and then it assists with due diligence."
(Participant 7)

Participant 12 identified that ISO 27001 has played a key role in addressing changing privacy laws with a risk-based approach that allows organizations to identify and mitigate risks in the processing of personal data while improving compliance with regulatory requirements on an ongoing basis. Additionally, Participant 2 mentioned that risk management is significant for the assurance of privacy complaints. This was corroborated by Participant 7, who opined that ISO 27001 certification had created a difference in their organization in risk management by aligning it to international standards, consequently improving privacy compliance and data governance. A further consolidation of these opinions illustrates how the ISO 27001 enables the management of privacy risk through defined controls, a process of continued improvement, training, and security controls that directly assist in preventing personal data breaches.

4.4.2 Continuous improvement and Learning

Continuous Improvement is a part of ISO 27001 since the ISO standards evolves overtime. Participants mentioned continuous improvement as one of the main learnings as well as benefits that will ultimately add to the company's overall information security process. Following are the extracts that were extracted from the interviews.

"Whenever you are faced with an incident you have to disclose with supervisor authority and they might see you in a manner that you haven't applied these properly and then they ll have to incur some money in to credit control and what not. It is better to implement isms in order to prevent those."
(Participant 1)

"Continuous improvement is a key part of ISO standards"
(Participant 15)

"Accountable people in the organization are using it to steer their security and steer their privacy, but make sure that it's a self-contained and improving system. So again, continuous improvement is a core component. So the benefits the discipline of the isms is, if you're following the methodology, you have a steering committee, you have continuous improvement, you have risk reviews."
(Participant 11)

"Decisions done too late in the process, which Then delays the whole project even more, and that's costs. So if everything is done in the right place and right moment, then it's beneficial for the company. And my understanding is that we, if we have this certificate, that was my wish, at least. And I feel that it could be done, that there is it creates and assess, that we have these processes and controls in the processes."
(Participant 10)

Continuous improvement is at the core of the ISO standards, which affect organizations in gradually enhancing their security, privacy compliance and effectiveness (Participant 15). An ISMS essentially acts as a safeguard used to prevent incidents occurring that would later bring an organization under the scrutiny of a supervisory authority, out of which any reputational or financial damage would arise. For an organization, having an ISMS in place for proactive risk management is the name of the game, where good corporate governance plays an integral role (Participant 1). ISO effectively creates accountability in this context, namely, very mature organizations that duly implement ISMS frameworks to ensure that security and privacy are steered by responsible people who also steer an independent and self-evolving entity. This elaborate procedure- made up of steering committees, cycles of continuous improvement, and risk reviews- would ensure an added level of discipline within the organizations (Participant 11). On the other hand, timely decision-making must occur since any delays resulting from security and privacy implementations can lead to project disruptions and/or escalation of costs. Having well-understood processes and controls is a significant way for the organization to boost efficiency and limit consequential setbacks in its overall risk management strategy (Participant 10).

4.4.3 Customer Trust

Customer Trust and Loyalty is one of the key aspects of maintaining a reliable customer base. Many interviewees emphasized how customer trust represents an important aspect of ISO 27001. The following are the relevant extracts and explanations for this.

"When we were trying to pitch customers, we could say your data will be kept secure. Here is our ISO 27,001 certification... it shows that we have met the stringent requirements... it's not just our word, it's somebody else's word."
(Participant 1)

"If I am a client, and I see a potential supplier has ISO 27001, I know that I wouldn't need to audit them. I know that someone else is auditing them to that standard, that they're having regular audits, that they're being checked out for these things."
(Participant 10)

"It's easy to show the paper saying we are ISO accredited... Instead of saying we take privacy and security seriously, here is this stack of documents that state why we take it seriously... Don't believe us. Believe this credited organization."
(Participant 11)

"Customer perception? That's the most important thing. Customers see us as a trusted partner... This certification is accepted worldwide. It opens the space for us to talk business, and we become like one army when it comes to protecting people's data."
"General awareness of every employee improves, and when that improves, privacy by design and security by design become default. This helps ensure privacy is built into the company culture, benefiting both internal security and external customer trust."
(Participant 6)

ISO 27001 certification contributes greatly to developing customer trust because it gives an independent verification of the organization's commitments in the areas of security and privacy. As per Participant 1, rather than bombarding the customers with volumes of documentation, an ISO certification would be the simplest and most credible way to show compliance and commitment to security. This was echoed by Participant 6, saying that the certification helps position the organization as a trusted partner in business discussions and provides a basis for a stronger relationship, knowing that data protection is a mutual priority. Similarly, customer reliance on ISO 27001 was echoed by Participant 10 as an assurance that fewer audits are needed because they know the other party is regularly subject to scrutiny from outside their own organization protocols. This was also related to Participant 11's view, which held that ISO 27001 not only ensures compliance but also incorporates security and privacy into a structured and continuously improving system reinforcing accountability. Further, participant 6 noted that

ISO 27001 promotes a security-aware culture within an organization, ensuring privacy and security by design default principles, thus further entrenching internal and external trust. All these views begin to show how ISO 27001 could enhance credibility while simplifying communication about compliance and creating trust that could last a long time with customers.

4.4.4 Improved Data Governance

ISO 27001 is critical for increasing data governance within an organization by providing an organized framework in the management of personal data. Implementers talked about the primary benefit of implementing ISO 27001 in terms of managing the personal data lifecycle, automating retention policies, and AI-assisted documentation that remained free from manual efforts and strengthened compliance. Below are the extracts from the interviewees that support this code.

"We have improved personal data lifecycle management... we have good processes privacy by design... retention periods are automated... the whole lifecycle management is taken care of... legal aspects are integrated, minimizing manual effort with AI-assisted documentation."
(Participant 10)

"Benefits include improved data governance, streamlined risk management processes, enhanced trust with stakeholders, and the ability to demonstrate compliance with multiple regulations through a single framework."
(Participant 12)

"ISO 27001 has strengthened our data governance framework, reduced the likelihood of data breaches, and streamlined compliance audits. It has also improved risk management by providing a structured approach to identifying and mitigating threats to personal data."
(Participant 14)

Several participants explained how much data governance is improved through ISO 27001 in their organizations. Participant 10 remarked that personal data lifecycle management had improved: *"privacy by design is embedded from start, and there are automated retention policies and AI-driven documentation which minimize manual efforts."* In support of this, Participant 12 stated that improving data governance fast-tracks efforts in risk management and compliance while enhancing trust with stakeholders. Similarly, Participant 14 stressed how ISO 27001 strengthened the data governance framework by decreasing the likelihood of data breaches and making compliance audits easier as it takes a structured approach towards identifying and mitigating the risks. Altogether, these findings prove that ISO 27001 can enable

organizations to have efficient and automated data governance practices that will comply with and ease the operational burden.

As per the participants, ISO 27001 implementation has several benefits for privacy across several dimensions. Improved Risk Management would be a foundational layer on which organizations bolster their personal data breaches by enforcing risk controls with Multiple-Factor Authentication (MFA), role-based access control, and pseudonymization, ensuring that the privacy risks are identified and addressed pro-actively (Participant 1, 12, 2, 7). Continuous Improvement and Learning also became an important aspect of ISO 27001 by creating an attribute of accountability, conducting risk reviews, and making proactive decisions to improve privacy compliance and security resilience (Participant 1,15,11,10). Certification has also enhanced Customer Trust, with organizations deploying ISO 27001 as independent validation of their privacy commitments, thereby increasing transparency of compliance and reducing the due diligence burden on customers/buyers (Participant 1, 10, 11, 6). Lastly, according to the interviewees, improved data governance has been furthered by automating the data lifecycle management, retention policies, and compliance audits. (Participants 10, 12, 14). Altogether, these insights show that ISO 27001 is more than simply a means of compliance. It has also become a strategy that organizations can adopt to mature their privacy practices and risk management while building trust across several stakeholders, thereby creating a balanced business environment concerning privacy-imposing strategy.

4.5 Theme V - Tailoring the Compliance Suit

Tailoring compliance refers to the process of identifying the regional challenges and evolving privacy regulations in the USA, Europe and China. The interview extracts under this theme have been categorized into six codes. They are the dynamic Nature of Emerging Privacy Laws, Gap Analysis and improvements, Lack of measurable Privacy Outcomes, Region-specific challenges and localization requirements, regional adaptation, regulatory overlays and contextual customization. In this section, the relevant extracts under each code will be explained.

4.5.1 Dynamic Nature of Emerging Privacy Laws

The landscape of emerging global privacy laws is a challenge to organizations in terms of compliance across jurisdictions. According to participants, various approaches among regulations, such as GDPR versus CCPA versus China PIPL, require region-specific compliance frameworks. ISO 27001 provides strong foundations in terms of security; however, it lacks detail in terms of privacy guidance and requires organizations to be complemented with legal reviews and risk assessments. The relevant extracts for the code are as follows.

"I'm very confident when it comes to the GDPR. In the case of the CCPA, they follow NIST because they're in the U.S. In China, they have their own regulations. When you read the PIPL, it includes its own security requirements and references. As a matter of fact, if I remember correctly, China doesn't have the same kind of Data Subject Rights (DSRs) as the CCPA or GDPR. Basically, they have access and rectification rights, as I recall."
(Participant 1)

"For example, this control for privacy… It says that follow the previous privacy legislations that apply to you… it doesn't go into details… it should be more detailed level guidance."
(Participant 10)

Above, participant 1 states the variability in global privacy laws. The approach of each regulation is different, even though the primary focus is data protection. The GDPR expert explains that it includes comprehensive data subject rights (DSR). According to PIPL China, however, the rights of access and rectification are limited. Participant 1 explains that organizations should prepare compliance frameworks that accommodate such distinctions to fulfil region-specific obligations. Participant 10 stated that the regulation provided in ISO 27001 is too generic and makes it difficult for organizations to put in place specific compliance controls. So, 27001 provides security frameworks; however, the privacy-related requirements may be too general. The expert emphasizes that filling such gaps is essential.

"A core component of the ISMS, again, is looking at applicable legislation. So, if you can see where that applicable legislation is applied, then you can connect the ISMS to privacy law. Privacy-related regulations incorporate cybersecurity—again, a core component.
So, regarding how it's affected by other legislation or privacy laws, the way that I approach it is by reviewing those privacy laws, looking at the specific security requirements, and then identifying the gaps in the ISMS"
(Participant 11)

Participant 11 states that Privacy compliance is not achieved solely through security standards and standards such as ISO 27001 would form a strong foundation, but businesses should always

go above and beyond any baseline security measures that may be available to address privacy requirements. This includes legal reviews, risk assessments, and other safeguards beyond technical security controls.

"New privacy laws are being introduced globally, with several jurisdictions updating their frameworks—such as Japan, South Korea, and Brazil—often in ways that align with GDPR principles. According to the participants, organizations that are already confident in their GDPR compliance typically find it easier to adapt to these types of regulatory updates. However, challenges arise in jurisdictions that adopt a significantly different regulatory path—particularly those with stringent data localization requirements. For example, countries like China and Vietnam require local storage and processing of data, which imposes additional compliance layers not explicitly covered by ISO/IEC 27001:2022. In such cases, ISO certification alone may be insufficient to demonstrate full alignment. Additionally, evolving national security-driven data laws, such as the U.S. Protecting Americans' Data from Foreign Adversaries Act, introduce restrictions (e.g., prohibiting transfers to certain nations) that go beyond the scope of what ISO/IEC 27001 addresses."
(Participant 4)

Participant 4 explained in detail the evolving and regionally diverse nature of emerging privacy laws. They noted that many jurisdictions—such as Japan, South Korea, Brazil, and India—have recently updated their privacy laws in ways that reflect key principles found in the GDPR, such as accountability, data subject rights, and data protection by design. According to the participant, organizations that are already aligned with GDPR tend to find it easier to adapt to these kinds of regulatory environments.

However, the participant also highlighted significant challenges in jurisdictions that enforce strict data localization rules. For example, some countries require that data be stored and processed within national borders, creating compliance obligations that go beyond the validation scope of ISO/IEC 27001:2022. They further noted that geopolitical developments—such as the U.S. Protecting Americans' Data from Foreign Adversaries (PAD) Act—introduce specific national security restrictions on data transfers to certain countries. These are not typically addressed within ISO/IEC 27001's general framework, making it necessary for organizations to consider supplementary legal and contractual mechanisms.

This reinforces the need for evolving compliance strategies that account for both technical standards and local legal landscapes. While ISO 27001 provides a strong security baseline, it cannot, on its own, guarantee privacy compliance across all jurisdictions—particularly those with localization mandates or politically driven data restrictions. Organizations must therefore

remain agile, continuously monitor legal developments, and implement tailored solutions where required.

4.5.2 Regulatory overlays and Contextual Customization

While changes in the landscape of national privacy systems certainly will prompt changes in policies and practices to meet ISO 27001 requirements, in practice, this can be a challenge. For example, while the GDPR sets very direct and particular requirements about encryption and risk assessments for each organization, CCPA has a more observer role toward consumer rights than a single target regulation. PIPL puts strict controls on data transfers, highlighting differences in approach. These are base discourses stressing that one model cannot suit all parties in matters of privacy compliance as there are other conditions put by national regulations, sectoral requirements, and other data protection authorities. The below extracts explain this dilemma in detail.

"The various regional laws pertaining to privacy have a bearing on ISO 27001 implementation projects. Europe's inclination is towards encryption and risk assessments for GDPR compliance-focused activities. In addition to that, the CCPA in America places attention on consumer rights access to require data access arrangements that are strong. PIPL is quite strict on the cross broader data transfers and China is quite serious about it"
(Participant 9)

This extract indicates the differences across regions regarding the implementation of ISO 27001 with respect to privacy compliance. It has been said by experts that even though encryption and risk assessments are very much vital in securing personal data under GDPR, in the case of the other regional privacy laws, like CCPA and PIPL, they have enforced other measures for addressing the data transfers across borders, where more emphasis is given to the data transfers in place of the risks. The expert has also mentioned the CCPA, saying that it is applicable to consumer rights, where rigorous data access mechanisms are required.

"There may be specific security requirements, which are a component of the privacy legislation that you need to adapt to modify for each country. So if you're looking at a country specific implementation of 27,001 it will differ. But as I say, in the ideal world, you bring it to the highest standard of whatever country it is that you're operating in requires that highest standard The answer is, the ISS will vary based upon each country, based upon each privacy requirement, based upon the technical requirements of the organization and the technical requirements of the regulators."
(Participant 11)

Participant 11 stresses that it is not suitable for the organizations to assume a one-size-fits-all policy with regard to privacy compliance. Each country has its expectations for security and privacy, which must be considered in the compliance strategies. This implies that even following ISO 27001, the implementation of which varies from jurisdiction to jurisdiction and requires modifications according to national laws, sectoral regulations, and regulatory expectations, an organization must abide by this approach to privacy compliance.

"Privacy and the regulations are rapidly changing and evolving… Even though there is one article in GDPR, it can be interpreted very differently in countries, and it takes a long time to get a decision on even basic interpretations. In Finland, privacy-related policies are included in more than 600 laws."
(Participant 10)

Participant 10 mentions even within the same regulatory framework such as GDPR, the interpretations can still have some differences from country to country or from professional to professional. National Data Protection authorities also can take different stances on legitimate interest, consent management and data subject rights. Participant also mention even in Finland there are more than at least 600 laws regarding privacy which explains the local authorities may pose additional requirements on top of GDPR. This proves the importance of contextual customization and regulatory overlays in the regional specific laws including the same law within European union.

"There can be differences in how the GDPR applies. Once I remember we came across that in Germany employers generally need explicit employee consent for monitoring due to ***strict*** *labor laws and the strong role of the Works Council****.*** *But in France, employers can rely on legitimate interest****,*** *though they must first consult employee representatives and provide a clear justification****.*** *This difference exists because GDPR allows Member States to impose additional conditions on data processing in employment contexts under Article 88. These subtle differences do not really impact ISO 27001 in my opinion.****"***
(Participant 2)

The participant 2's discussion is largely about regulatory overlays as well as contextual customization governing how compliance with the GDPR changes across different EU Member States. Article 88 empowers national laws to attach additional conditions to the processing of personal data relating to employment and therefore leads to differences even in the application of the common legislation: For instance, the following examples are enough to illustrate these differences: Germany's strict labor law and Works Council influence require providing employee monitoring under conditions of explicit consent, while France permits monitoring

under legitimate interest but following consultation with employee representatives. Thus, these differences would mean that the organizations must customize their compliance strategies to fit local labor laws and regulatory interpretations. ISO 27001 remains largely unaffected due to these nuances- while it points to security, not legal de facto justifications, the organization must also accommodate its data governance practices to safeguard privacy-compliant operations in each jurisdiction.

4.5.3 Lack of measurable Outcomes

Lack of measurable outcomes refers to a key challenge in privacy compliance is the absence of standardized and quantifiable measurements for assessing the effectiveness of privacy initiatives. Many organizations use ISO 27001 or their country's regulatory compliance frameworks; privacy regulations, however, continue to demand additional measurable outcomes, sometimes outside the organizations' direct control, such as data subject rights requests, responsiveness to breach incidents, or privacy risk assessment. Extracts follow to evidence the above challenges.

"GDPR actually requires that we can give authorities the number of data subject rights and requests, and at the moment we don't have those numbers. There's no system to gather all that data, so if it's not built from the beginning, it's hard to go back and create those measurements." (Participant 10)

This illustrates how it becomes a dilemma for organizations without keeping a tab on privacy metrics, although the same GDPR requires reporting relative to data subject rights requests. Without having a structured framework for assessing performance on privacy issues, such companies may find it hard to prove their compliance when asked by regulators. Privacy KPIs are not found, unlike security frameworks that emphasize encryption or access controls. As a result, it is hard to gauge compliance maturity.

"We haven't had any good key performance indicators, or we haven't, maybe measured our maturity. But I would say that that's the that's the direction that we are going to, and that's also good thing in the standard that it is forcing you in the mode of continuous improvement. I think that's also a learning point that how much are we able to improve in a year. Identify your things and remediate so forth, and what can be put later on the roadmap." (Participant 13)

Participant 13 mentions that in their experience they had not had key performance indicators measured for privacy maturity. Also, they emphasize that the standard although focuses on continuous improvement. However, in their opinion it does not convince enough that ISO 27001 provide measurable outcomes for privacy compliance.

"An ISO 27001 auditor will ask how many incidents you had, but that doesn't tell the whole story. you could have one incident, but it could be we suddenly have access to 100,000 people's financial and biometric data, or it could be one incident of somebody sending the wrong email to somebody else. Both, from a binary point of view, are a data breach. One is up here. One is negligible. ISO is more qualitative than quantitative in this regard."
(Participant 4)

ISO 27001 has provided many quantifiable outcomes. It has improved our breach detection time by 40%, meeting GDPR's 72-hour notification requirement. Also, by implementing encryption controls reduced incidents of unauthorized access by 25%.
(Participant 14)

However, participants 4 and 14 both state that implementing ISO 27001 has provided measurable outcomes. Participant 14 specifically mentions that their breach detection time improved by 40% and incidents of unauthorized access controlled by 25%, which is highly relevant to privacy as well. Participant 4 agrees that it provides measurable outcomes; however, they emphasize the numbers can often misguide since a breach can be relative to the amount of data and the significance of the impact. At the same time, there could be occasions where unauthorized access did take place. However, the impact was quite small. In Participant 4's view, they think that ISO is more qualitative than quantitative.

4.5.4 Gap Analysis and Improvements

Organizations in the different landscape of cybersecurity and privacy regulations are facing both opportunities and challenges in managing ISO 27001 (Information Security Management System, or ISMS) in a way that aligns with privacy frameworks such as GDPR, PIPL, or other regional laws. A gap analysis points out important places where the ISO 27001 framework fails to distinguish between the important new privacy needs and suggests tactical fixes. By combining ISO 27701, regional risk assessments, and better privacy governance structures, organizations will then be able to create a compliance framework that protects their data.

"There are gaps. Yes, one of the gaps I identified was ISMS Protect all the data while privacy protect all the personal data. Personal data has identifiers. So, ISMS has a broader vision and

sometimes they simply think having a password and multifactor authentication is enough anf privacy people think if the pw is stolen what then? And am I revealing too many personal data or identifiers. Security folks be like this is enough. Privacy folks like rights and freedom. Security folks would not think that way as a human right. Even if I go back and say if a pw is stolen you are in a privacy risk and then make a stronger pw policy again. the risk that I am posing as a privacy has always a solution in security. The depth of understanding the repercussions of the risk is shallow in comparison to privacy with security."
(Participant 1)

These extracts of Participant 1 shows the fundamental gap between ISMS and privacy protection. ISMS intends to protect all sorts of data; privacy only focuses on those data with identifiers that are personal. Security professionals usually take internal technical views (e.g., passwords, multi-factor authentication), while privacy professionals look at broader aspects of human rights (e.g., data minimization, consent, data subject rights). This distinction is crucial in respect of building compliance frameworks organizations should embay privacy into security rather than treat them separately.

"I said at the very onset, it's a system of your own making. If you address the requirements and you expand the requirements, so going to GDPR as prime example, if I go to the UK NHS and they have something called the DSP. DSP is the digital security profile the toolkit for me. Measuring compliance to privacy and to security. When you complete the DSP, if you've got ISO 27,001, they consider that you've met the requirements of the GDPR. You may from a technical security perspective, but you've not met the requirements of the GDPR because of GDPR, if you look at, for example, Article 28 it's a series of contractual measures, series of contractual positions, supplier, surveillance, technical measures, technical measurement, and then security overlays. So, going to does ISO 27,001 help you meet those standards? It does if it's implemented correctly, but there's a lot more work to do if you're just looking at it in isolation, then the answer to me is a clear No."
(Participant 11)

According to Participant 11, ISO 27001 may help meet GDPR obligations. However, it is not totally adequate on its own. It adds requirements for contracts, governance, and supervision related to GDPR, including DPIAs and supplier management, when security controls alone will not be adequate. It is important to avoid misleading organizations into believing that obtaining ISO 27001 certification equates to GDPR compliance. Thus, more controls are required, particularly in areas like privacy impact assessments and third-party risk management.

"We have completely different or our privacy kind of governance structure uses the same governance structure than the security governance in the organization, because the security governance was the first and it would it made sense to apply the same governance structure on the COVID level, but then we have also this kind of do of local privacy champion network, where we kind of make sure that We understand each other. But otherwise, I think, personally,

I think that there are huge gaps between privacy laws and ISO 27,001 and we have a separate organization taking care of those kind of privacy requirements in privacy, privacy laws as such, and ISO 27,001 is also a helpful standard to make sure that the security controls are in place." (Participant 2)

Integration of privacy governance into established security configurations poses certain problems. Many organizations start with some security governance framework and later try to bring it up to speed with privacy requirements. While harmonizing privacy with security governance may have its benefits, usually there are additional skill sets and governance for privacy matters. Assigning local privacy champions across business units may aid in understanding and implementing privacy regulations. Organizations must recognize that ISO 27001 can never be the stand-alone standard for privacy and therefore would require independent privacy governance.

4.5.5 Regional Adaptation and Localization Requirements

Adapting to the emerging global privacy regulations, organizations will adopt maybe a distinct compliance strategy for GDPR, CCPA, and PIPL. Certainly, ISO 27001 finds a robust application for establishing the framework for information security, but none of these can be exclusively made to guarantee specific legal compliance with any of these regional privacy laws, as they include various duty requirements with regards to data subject rights, cross-border flow of data, and consumer protection. The requirements of each region will leave ISO 27001 short as far as compliance is concerned; therefore, businesses will tailor additional controls for encryption, data localization, and transparency to cover jurisdictional requirements. This section brings to the fore the challenges organizations will face in refining their security and privacy practices to meet the nuances of regulations across Europe, the U.S., and China.

"CCPA is mostly like 80% GDPR. They have copied 8-% of GDPR and made it liberal. In GDPR for an example the cookie consent, is like someone has to come and effortmetly have to say yes in order to opt it. California like you already is opted in you have to specifically opt out."
(Participant 1)

This creates a significant difference between the cookie consent mechanisms adopted in the GDPR and CCPA. Under the compliance in the GDPR with cookie and tracking technologies, upfront opt-in consent is a requirement whereby users must actively give consent before data

is collected. By contrast, CCPA adopted an opt-out approach, with users now being given an option to opt out of the sale of their personal data, without specific opt-in conditions for cookies. The practical difference of these two approaches might be, they are more valuable for organizations that have operations across regions as they would have to put different systems in place for stricter opt-ins by GDPR requirements, and still address the opt-out model under CCPA for the consumers based in United States.

"From a privacy perspective, privacy laws vary, but if I give an example of the United States, I'm working at the moment on a privacy notice for a client in the United States. They are implementing employee monitoring. And if you consider U.S. state law, there are six states in the United States that require you to manage employee monitoring and notify employees. The other states, they don't really need that. But just using that in isolation, if you look at California, in California, there's a requirement to notify any third parties. Notify your employees of any third parties that you're using. That is a prime example of variation. In regard to privacy, you have to consider the applicable law, and you have to consider best practice. You must consider the context of the organization and its international outlook."
(Participant 11)

This highlights common challenges in complying with the Personal Information Protection Law of China. With regard to data localization and cross-border data flows it is stressed that China is quite strict as there is no such transmission unless endorsement from the relevant Chinese regulatory authority is received by the organization. Whereas, every law has its condition on cross-border data transfers, the CCPA being consumer-right oriented, GDPR takes on complicated legal procedures such as Standard Contractual Clauses (SCC). In addition to more stringent local transfer rules ISO controls can offer a sensible starting point for putting the required safeguards into place Such investments will involve encryption, supplier audits, authentication measures, and processes to government regarding cross-border data transfers- all requirements from PIPL which businesses have in mind when dealing in or with China.

"The core principles of ISO 27001 remain consistent, but its application may vary. In Europe, organizations often focus on GDPR-specific requirements like data subject rights and data transfer mechanisms. In the U.S., there's more emphasis on breach notification and consumer rights under CCPA. In China, the focus shifts to PIPL's stringent data localization and cross-border transfer rules."
(Participant 12)

Participant 12 reflects on the regional variations of the focused fields in privacy compliance: GDPR (EU): The main focus has been given on data subject rights (access, erasure, portability) and cross-border data transfer mechanisms (Standard Contractual Clauses, Binding Corporate Rules) CCPA (U.S.): The major area of focus is on breach notifications, opt-out rights of

consumers from sale of data, and mandatory disclosures PIPL (China): Introduces strict data localization rule and seeks prior approval from the government for transferring the data outside the country, making compliance much more stringent than GDPR or CCPA.

Derived from compliance strategies tailored for regional privacy laws, organizations must draw the line between compliance with ISO 27001 and jurisdiction-specific needs. Generally, ISO 27001 is presumed to be a sound assumption for security. However, the other side is that actual compliance seems so full of nuances with respect to global privacy regulations that it may be outright difficult or impossible to apply GDPR, CCPA, and PIPL. Yet since business models are continuously evolving, the other obligations, the layers of regulations on top of others, and the evolving legislation will periodically call for adaptations and engagements in legal reviews. Governance of security must also be integrated with privacy, and the context of compliance must consider local expectations and measurable outcomes. A one-size-fits-all approach is ultimately unsatisfactory, and organizations will have to evolve their compliance frameworks/designs to fit the styptic letter of evolving international standards.

In order to comply with jurisdiction-specific standards, enterprises must modify their compliance methods beyond ISO 27001 to accommodate regional privacy legislation. Despite providing a solid security basis, ISO 27001 falls short in addressing the subtleties of international privacy laws like the CCPA, PIPL, and GDPR.

4.6 Theme VI – Future Proofing the Shield

The 6th and last theme is Future Proofing the Shield, which specifically focuses on the future perspective from the experts. The Futures Perspectives were coded under this theme in 3 different codes. The coding was arranged according to the relevant interview extracts as well as the questions that were asked by the experts (refer to the appendix 1 for questions). The three codes are ISO 27001's Future, Trends and Best Practices and Future Proofing Compliance. The relevant extract and their explanations are as follows.

4.6.1 ISO 27001's Futures

"Even in India they recently coming up with DPDPA, they are also emphasizing the same 3 I mentioned above as confidentiality, integrity, and availability... One thing I would assume is AI. ISMS can be really improved on AI measures. Remember how they come up with cloud computing. 10 years back ISMS was on premises. Now they have extended their services to

cloud even. Similarly, they should come up with and I think they are on to it already and there is a need for AI now... Many orgs see the benefit of using AI but they are struggling to implement because they are not fully aware of the risks associated with it."

“One way to put is azure is offering you a personal tenant. There is a price model in azure cloud. They ll give you your own talent. If you implement ChatGPT or AI it will stay there and will not be shared. So how to build security in such scenarios that ISMS must really improve.” (Participant 1)

Participant 1 mentions the Technology transition from on-premises systems to cloud computing needs to addresses AI security measures through ISMS. While acknowledging the importance of AI to most organizations, the participant says that the major concern is how to use it safely for the reasons of being ill-informed about the risks. The participant even talks about securing AI models in a cloud environment, for example, within an Azure personal tenant system and implies that the ISO 27001 should change the standard prescriptions to include particular security issues regarding artificial intelligence.

"I think the biggest problem is what I mentioned about AI... With AI, what I'm seeing is more abstraction and an AI layer leading to business logic... With AI, you've got the truth, you've got a half-truth, and a lie."

"If you consider security, the problem to security is that you have to understand your data. You have to classify your data. So going to an ISMS, if you don't understand the data that you have, you haven't classified that data, and you've got no security."

"ISO 27001 hasn’t taken into account the requirements of AI... If you’ve not classified your data, you can’t protect it... The biggest challenge to AI is that if it's learned something that it shouldn't have learned, you can't make the AI unlearn that."

"ISO 27001 needs to change and adapt. It has to take into account AI systems. And what we have to do is look at a more comprehensive toolset, covering privacy, covering cybersecurity, and considering the integration of AI."

"The ISMS, as it currently stands, deals with more traditional-based technology systems. And I would argue that when it comes to cloud-based systems and software as a service, so isms need to evolve, to factor all of those areas."
(Participant 15)

Participant 15 discusses with a critical approach toward AI's effect on ISMS. According to them, AI aggravates security because of the introduction of some risks, such as misclassification of data and the inability to "unlearn" sensitive information. These new challenges are consequently complicating CIA, which inter alia makes ISO 27001 work. Contrarily, the also explain that the current ISMS model is not really fit for purpose given cloud

and AI systems and calls for a wider set of tools towards a more integrated notion of AI security, privacy, and risk management.

“Maybe it would be more relevant to even discuss about the whole 27,000 series. Yeah, 27,001/02 is the password that everybody is talking about, because it's like the vast majority of the work, or the effort that you are concentrating on from the data protection perspective. But if privacy is more relevant to your organization and it's more critical in your business, then maybe you are if you look at the standard set and the 27,000 series, then maybe you take that 27,007 and 27701 in your toolbox.”
(Participant 13)

Participant 13 argues that the focus on ISO 27000 series is needed instead of ISO 27001/02. In their point of view, they highlight that ISO 27007, which specifically focuses on ISMS auditing, and ISO 27701 PIMS are potential valuable additions for organizations where privacy is a key concern. Their viewpoint suggests companies should use the additional standards to address privacy as well as security comprehensively.

"You'll see either entirely new standards come out and the 27,000-suite rendered obsolete, or you'll see 27,000 added to, so you'll go with ISO/IEC 42001*... You won’t see 27,001 changes much."*
"At the moment, it is AI, as you are well aware. AI is already revolutionizing security… AI is being used for phishing techniques or social engineering techniques… You could see rises of synthetic data again, how well it’s been made. You can see so many different things that can happen with AI technologies that will affect ISO standards going forward."
"You could even see ISO itself changing—an auditor could literally just be an AI system… The potential for AI will change so many things in security and privacy, both from an administrative point of view, from a regulatory point of view, and even from a use case point of view."
(Participant 4)

Participant 4’s view on the ISO 27001’s is quite crucial in the findings of the interview. They point out two possible futures. 1) ISO 27001 will be completely obsolete and be replaced by a new standard. 2) It could continue through expanding through additional standards such as ISO ISO/IEC 42001:2023. Participant mentions the impact and emerging risks of AI. AI has been used for phishing and social engineering, as well as for synthetic data. The participant states that an important perspective is that in Future, an auditor may be completely an AI system. So, in the participant states, both from an administrative and regulatory point of view, Artificial Intelligence will have a significant role in the certification implementation of audits in Future.

"ISO 27001 can further be strengthened with privacy-specific controls, such as guidelines for data subject rights management, consent mechanisms, and principles of data minimization. This would remove the necessity for additional frameworks like ISO 27701 since companies

are heavily investing their resources in ISO 27001 and may not put as much emphasis on ISO 27701." (Participant 12)

Participant 12 states that ISO 27001 is purely about information security and not a normative approach to privacy controls. With the introduction of privacy governance characteristics like the rights of data subjects and consent, ISO 27001 may further ground itself as less reliant on other frameworks like ISO 27701. In addition, companies may be reluctant to invest in extensions like ISO 27701. Hence, this creates a need for a more comprehensive standard that would align itself better with security as well as global privacy frameworks.

4.6.2 Trends and Best Practices

Emerging technologies and regulatory challenges drive the evolution of ISO 27001. One key theme that surfaced in the interviews was whether ISO 27001 remains relevant or will soon be subsumed by another standard. Some see it going forward by windfall of new standards; others think an integrated approach is better, joining security and privacy frameworks. Privacy governance should remain a concern. Companies invest the majority of their resources in building Information Security Systems, whereas the concern for privacy is neglected or ill-noted. However, with the technological transformations taking place in workplaces, privacy has been a part of important discussions. The trends and best practices of this technology transformation are significant in understanding the ISMS and Privacy transformation. The following extracts will explain the trends and best practices of ISMS according to the experts about privacy.

"You'll see either entirely new standards come out and the 27,000-suite rendered obsolete, or you'll see 27,000 added to, so you'll go with ISO/IEC 42001*... You won't see 27,001 changes much."*

"At the moment, it is AI, as you are well aware. AI is already revolutionizing security… AI is being used for phishing techniques or social engineering techniques… You could see rises of synthetic data again, how well it's been made. You can see so many different things that can happen with AI technologies that will affect ISO standards going forward."

"You could even see ISO itself changing—an auditor could literally just be an AI system… The potential for AI will change so many things in security and privacy, both from an administrative point of view, from a regulatory point of view, and even from a use case point of view." (Participant 4)

Participant 4's view on ISO 27001 is quite crucial in the findings of the interview. This is also coded under trends and best practices as well since the two possible futures mentioned is relevant for this code as well. Participant points out two possible futures. 1) ISO 27001 will be completely obsolete and be replaced by a new standard. 2) It could continue expanding through additional standards such as ISO/IEC 42001:2023. Participant also stresses the possible impacts of AI in the areas that have emerging risks, including issues such as phishing attacks, synthesized data and audit security with AI. The interviewee's main argument appears to be how AI will significantly alter future security and privacy.

"There are article 29 Working Party papers that indicate or strongly hint that anonymization to the GDPR standard, and obviously to other global standards, is essentially impossible. You either anonymize it so much that any usable data from it is gone, or anonymization is being used in lieu of simply saying very high-level encryption plus pseudonymization. Anonymization has to be irreversible for a billion years, and it can't reverse that data, and essentially, that's almost impossible to prove. So, yeah, that's the other one. Is anonymization isn't possible in the way that people think it is. So that's the other technologies. If we can get full on anonymization approved by the edpb, that would also change things."
(Participant 4)

Participant 4 speaks here that GDPR and other global privacy frameworks set a higher standard for anonymization. To interpret GDPR requires the data to be irreversible for an indefinite period. However, as the Article 29 working party papers (Now EDPB Guidelines) indicate, achieving true anonymization is almost impossible. The participant states that if the data is anonymized to that standard, the usability of such data is lost. Many organizations use high-level encryption and pseudonymization instead of true anonymization anyway. However, it has the possibility to re-identify and hence would not meet the GDPR anonymization threshold. From the best practice perspective, organizations should be cautious about relying on anonymization as a compliance measure. Instead, strong encryption, data minimization, and access controls should be installed as complementary safeguards.

"You need to be careful what AI tools you use. I'm very fortunate that the company I work for has its own internal chat GPT, 4.0 which is a safe environment to plug information into, but it's a very good way to test things. So for example, you can take the GDPR, attach that as a document into this chat GPT model, and then you can submit your data minimization scheme or your data security documentation and say, compare is this compliant? And it will spit out the answer. So that is something that can be utilized more obviously, it's a case of trust but verify so whatever the GPT spits out, question it. No, don't, don't take it. Word for gospel. You need to question it. You need to verify it. But it's a great way of cutting down a lot of the review time. So that is definitely the single emerging technology that should be focused on. Otherwise. The only other one is and this isn't necessarily an emerging technology, but it's something that

should be taken into consideration. Our privacy enhancing technologies (PETs), patents, a lot of them don't show privacy compliance in that way, a lot of them simply show steps being taken towards compliance. Compliance is a moving train. It's a moving target. But things like federated learning, for example, is a great way of demonstrating that you're moving towards this ISO standard, that you are taking privacy and security seriously"
(Participant 4)

Participant 4 explained how to organize their own internal AI models, such as ChatGPT 4.0, to automate compliance checks for the companies. This would very much reduce the reviewing time by running the data minimization or security policy through AI evaluation. Although compliance efficiency is enhanced, it should not be trusted blindly. Organizations must verify their outputs to ensure accuracy and bias. This speaks to a broader topic where human oversight should not be overlooked by the efficiency of AI. Another emerging best practice is Privacy Enhances Technologies (PETs), which demonstrates an organization's commitment to privacy and security. Compliance, as it stands, is a moving target, and the PETs will help an organization align with both ISO standards and regulatory expectations. It is also mentioned as ensuring continuous improvement over static compliance, which means being more attentive towards improving along the work of compliance rather than only trying to complete the regulatory obligations. Organizations can integrate AI and PETs into their security framework and better place themselves for future changes in ISO 27001 and regulatory provisions.

"It is about education and benefits. Going to what I said about the challenges to implementation. Lots of organizations see it as a financial burden. It is, but that burden can be offset by the benefits if you understand those benefits. So, it's about educating people as to those benefits, and if they're educated, they'll understand and hopefully start moving towards that. Best Practice, even if you get a third of the way there, then you're a third of the way ahead of many organizations who are just implementing a standard as a tick box exercise. So, education and understanding are core components, and that has to be organization wide. It has to be vertical as well as horizontal. What I mean by vertical? Educate your customers, educate your suppliers, and go across the organization. When you factor those and start considering things in the security and privacy context, then you're tending towards best practice. It starts with an idea and sharing ideas. When those ideas are shared and developed, that's where you get best practice"
(Participant 4)

For the implementation of ISO 27001, the top priority should be imparting education and awareness across the organization. Some organizations view compliance simply as a cost, merely another tick on a list of requirements. Organizations that appreciate the benefits of compliance beyond escaping penalties will probably embed security and privacy into their culture. Education is a big enabler in changing that perspective. The more companies can

educate their employees, suppliers, and even customers on security and privacy requirements, the more they are inclined toward adopting real best practices instead of rigid checklist approaches. This should be vertical and horizontal compliance knowledge that flows top-down from leadership to employees but will also go out to partners and stakeholders. The essence of best practice is dialogue and free-flowing ideas, which means security and privacy are de facto cultivated and improved rather than grudgingly adhered to. Likely, these organizations that prioritize education in security and compliance rather than just an annual training session will incorporate security into their operational fabric and keep abreast of compliance hurdles as they evolve.

4.6.3 Future Proofing the Compliance

The "Future Proofing the Compliance" code was related to the advice that was given by the experts in the future for companies who aim to align ISO 27001 with future privacy requirements. The extracts below explain how this code was supported by the extracts and what their advice is for companies that wish to combine ISO 27001 with Future Privacy Requirements.

"In future, ISMS right now as it is I see take care of the data protection part. With AI they will have to come up with stringiest standards. Other than simply implementing the standards or should minimize the data and only collect what they want. No matter how strict the security there is nothing 100% perfect. You end up losing the data even in strictest systems. Data minimization should be focused on. Other thing I see is that not having a proper retention policy. It is part of the ISMS too. And don't be a data holder. You must let go. Without having any feelings attached to it the data should be wiped out. Sometimes marketing fokes would dig 3 years old data and try to reinvent leads. But hey the world is changing and may be those data is not even valid anymore. So you have to put some practical thought and decide we have a robust retention policy along with a string ISMS practice."
(Participant 1)

Participant 1 advice the rise of AI and the importance of stringent standards to protect data. It is also mentioned that data minimization and it is not practical to implement 100% systems. Every system may have flows. Further, it is emphasized that proper data retention times and holding data longer than needed are not emphasized. Sometimes, this may take place in a marketing department for holding on to data more than they should. The participant emphasizes that by saying, "You have to let go". Overall, their advice is that the world is evolving and that practical thought is needed to decide on retention policies along with ISMS practices.

"I would say that they should map the requirements of both standards, so that once they map the requirement of both standards, they can see that, okay, once I achieve this, then this one, for example. So I achieve this on ISO standard, then it's done in my own privacy law once I achieved it, and I just let it start, but and then at the end of it, they will be able to notice the gaps and individual tasks that they need to fulfill both for both laws. So I think, yeah, data standard mapping is a very good place to start."
(Participant 7)

According to Participant 7, mapping ISO 27001 requirements to other privacy laws and standards is the best practice for efficient compliance management. Companies would understand where requirements overlap and hence reduce their burden of compliance, as some requirements become redundant. It is mentioned that, ultimately, such systematic management of security and privacy obligations makes compliance more sustainable and manageable in the long term.

"I would tell them not to limit themselves to just the ISO 27001 standard. The legal requirements applicable to the EU and European economic area can be found in the GDPR. In addition, you may familiarize yourself with the ISO 27701 standard. It is extremely important to explore the risks to data privacy, security and data governance posed by the use of AI applications, and to understand the means to mitigate them."
(Participant 5)

"I think following ISO 27,001 I think it's a good idea, and utilizing the same kind of management framework for privacy compliance certainly is useful. I think the setup where you have legal department just kind of writing privacy notices and perhaps writing article 30 record records description probably doesn't work that well because legal department probably is a little bit too far away from the actual technical implementation, but I think security organization typically is closer to the technical implementation of the relevant systems. So therefore, combining those management system makes sense to me, and therefore, also it may be a good idea that those 27,001 and 27,701 are combined."
(Participant 2)

Participants 5 and 7 both states not to limit themselves to ISO 27001 and, go beyond ISO 27001 and familiarize themselves with ISO 27701. As stated in previous chapters, ISO 27701 is also a PIMS (Privacy Information Management System). Also, the findings show that expert advice is to focus more on risks related to data privacy because of the use of AI applications. They stress that the risks should be mitigated. The legal and technical departments should work together to achieve a common goal.

"I would say your top management needs to understand that this is their case, It is not CIO's responsibility alone. So, they have to understands it is their business and you need to keep the scopes really clear. If you don't. you will probably get a bloat, and you can't have ISO 27001. If top management isn't backing up, you don't have base to build on."
(Participant 3)

"I would endorse the approach that the management system should be lean enough so that you can do rapid enough changes. You should not have an excessive number of policies that make compliance overwhelming. If there are too many policies, people might not even be aware of them, or they won't know who is responsible for what. Ownership must be clearly defined, and those responsible must actively maintain it. If you have a massive management system or massive documentation, compliance efforts may start strong but fade over time. And when key personnel change, the ownership might drop, and the policies will be forgotten."
(Participant 13)

Participant 3 and Participant 13 both explain the importance of scoping and the simplicity of the procedure without making it overly complicated. Ownerships should be clearly defined in order to maintain the processes, and it is also noted that top level of the management should be involved in implementing ISO 27001 and the responsibility should not solely be on the IT team. To conclude, organizations should remain proactive rather than reactive on maintenance related to compliance with ISO 27001. This requires a focus on data minimization and retention policies that value risk mitigation, especially as it stands today with AI-driven security challenges. Education and awareness must transcend being a mere check-box exercise in compliance for the employees in the organization. A holistic approach can weave together ISO 27001 with ISO 27701 towards benefits both security and privacy management. Management should actively pitch for ISO 27001 to be considered a business function to support compliance. Upcoming issues such as AI risks and complexities in data governance, organizations will have to widen the scope of compliance beyond ISO 27001 and offer a cross-examination of requirements required by various standards and regulations. It is advised to focus on gaps and use unifying approaches. By adopting such strategies, organizations can future-proof their compliance programs so that their enduring capacity will always stand strong against growing regulatory and technological complexity.

Chapter Summery

Chapter 4, Data Analysis, consist of the findings from the interview conducted as the primary data collection method. There were extensive interviews conducted by 15 participants, and the extracts that were described are the findings from those interviews. The participants were

experts in data privacy and cybersecurity who worked in multinational companies with clients mainly located in the USA, Europe, and China. The location of participants was based in the EU, the US and Former Members of the EU.

According to the findings, the interviewees have had experience in the privacy and cybersecurity field. Participants included individuals who are very advanced and have over 20 years of experience working in the field of cybersecurity and privacy, as well as entry-level individuals who have 3 to 6 years of experience. Well-experienced professionals have gone through changes in the privacy laws established by countries and international standards like GDPR with increasing demand and dependency on ISO 27001. Even the limited experienced professionals have gone through the process of implementing ISO 27001 in their respective organizations.

The researcher primarily interviewed 17 participants for the data collection and decided to use the 15 interview transcripts that gave relevant finding for the research questions. 2 of the initial interviewees did not pose enough experience in the ISO 27001 implementation and hence the researcher used the data from the 15 participants who gave valid findings to fulfill the research objectives.

There are 6 main themes according to the coding process and below table represents the themes and the codes of the findings.

Table 4. Main Themes and Corresponding Codes Identified from Thematic Analysis

Theme	**Codes**
Building the Privacy Foundation	▪ Role and Responsibilities ▪ Experience with Privacy and ISO 27001 and Location ▪ How Privacy is built ▪ ISMS Contribution to Privacy Laws ▪ Evolution of Privacy Compliance ▪ Understanding of Privacy Compliance
The Privacy Security Bridge	▪ CIA: Integration and Alignment ▪ ISO 27001 as a Foundational Framework ▪ Privacy Relies on Security ▪ Insufficient for Privacy Compliance Alone

Breaking the Barriers	▪ Resource Requirement and Leadership Support ▪ Misalignment ▪ Organizational Culture as a Challenge ▪ Privacy Challenges due to Limited Scope ▪ Communication as a Challenge
Harvesting Privacy Gains	▪ Improved Risk Management ▪ Continuous improvement and Learning ▪ Customer Trust ▪ Improved Data Governance
Tailoring the Compliance Suit	▪ Dynamic Nature of Emerging Privacy Laws ▪ Regulatory overlays and Contextual customization ▪ Lack of measurable Outcomes ▪ Gap Analysis and Improvements ▪ Regional Adaptation and localization Requirements
Future Proofing the Shield	▪ ISO 27001's Futures ▪ Trends and Best Practices ▪ Future Proofing the Compliance

The Theme 1- Building the Privacy Foundation Theme discovered relevant findings pertaining to the creation of a strong privacy foundation for the added integration of security frameworks, for example, ISO 27001, to evolving privacy regulations. It has been discovered that ISO 27001 is an important place for establishing security controls related to privacy compliance, but it does not stand alone in satisfying legal and privacy obligations. Organizations are required to supplement it with governance measures that are specific for privacy and continuous improvement. The evolution of privacy compliance from being an initiative driven by regulation to a proactive embedded practice makes the understanding different. Ultimately, a well-structured information service management system under appropriate privacy frameworks will require a holistic approach that is legal, technical, and organizational.

The second theme, the privacy security bridge, explores that privacy does not mean locking away data. Privacy is about who accesses the data, how the data is used, and why it is processed. Since ISO 27001 was created for general information security rather than specific privacy-related requirements, organizations should use it in combination with relevant legal frameworks and align operational activities. Ultimately, the extracts highlight that privacy and security must work together to build a truly compliant and effective data protection strategy.
Third Theme, Breaking the barriers explores, to deal with this challenges, organizations need to stimulate cross-functional collaboration, invest in continuous training, secure full leadership

approval, and integrate additional frameworks focusing on privacy into their own ISMS. Failure to do so might very well reduce ISO 27001 into a mere compliance tool instead of a deep framework for security and privacy governance. Addressing these obstacles will help organizations establish an effective privacy-aware security management system, thus assuring compliance while buttressing data protection and risk management strategies.

Theme 4, Harvesting Privacy Gains focuses on the benefits of ISO 27001 offers. ISO 27001 has offered significant benefits for privacy by strengthening risk management, fostering continuous improvement, and enhancing customer trust. It helps organizations proactively address privacy risks through security controls like MFA and access management while promoting accountability through regular risk reviews. Certification also boosts transparency, reducing compliance burdens for customers. Additionally, improved data governance streamlines data lifecycle management and audits. Overall, ISO 27001 is more than just a compliance tool—it's a strategic framework that enhances privacy maturity, builds trust, and creates a balanced approach to security and regulatory requirements.

Theme 5, Tailoring the Compliance Suit - It has been argued that adapting compliance strategies to local privacy laws requires organizations to go beyond ISO 27001 and tailor specific jurisdictional requirements. ISO 27001 provides a well-structured security foundation. However, it misses the nuances offered by diverse global privacy legislation, including GDPR, CCPA, and PIPL. Dynamic emerging legislation, regulatory overlays, and localization mandates will require continuous realignment and legal reviews going forward. Compliance must be contextualized, plumbing privacy governance into security towards some measurable outcomes and regional expectations. Ultimately, a one-size-fits-all approach is insufficient, and organizations must find what is suitable for their industry and each business when dealing with compliance requirements.

Theme 6 was specifically added to identify the expert views on the future perspective on ISO 27001 and the regional privacy requirements. The experts emphasized that organizations should remain proactive rather than reactive in maintenance related to compliance with ISO 27001. This requires a focus on data minimization and retention policies that value risk mitigation, especially as it stands today with AI-driven security challenges. Above the technical measures, education and awareness are crucial for the employees of the organization to move beyond mere check-box exercises in compliance. A holistic approach that weaves ISO 27001

and ISO 27701 together can yield double benefits for both security management and privacy management. The management should actively pitch for ISO 27001 to be considered as a business function to support for compliance. Upcoming issues such as AI risks and complexities in data governance, organizations will have to widen the scope of compliance beyond ISO 27001 and offer a cross-examination of requirements required by various standards and regulations. It is advised to focus on gaps and use unifying approaches. By adopting such strategies, organizations can future proof their compliance programs so that their enduring capacity will always stand strong against growing regulatory and technological complexity.
The conclusion summarizes the main findings of the chapter 4. The upcoming chapter 5 on Discussion will Analise how the findings relate to the specific research questions and how it fulfills the research objectives.

Chapter 5
Discussion and Findings

This study aims to find out how ISO 27001 as an Information Security Management System (ISMS) can help organizations fulfil emerging global privacy regulations such as the GDPR, CCPA, and PIPL. Privacy and data protection-related regulations keep on evolving, and organizations are getting increased pressure to align their privacy and security framework to the corresponding security requirements. This study aims to explore how ISO 27001 contributes to privacy compliance, how ISO 27001 is applied in different regional privacy regulations and the challenges and benefits of implementing ISO 2700 by using three different regions, which are Europe, the USA (California), and China.

This research utilized thematic analysis to code and analyze interview extracts, aligning them with the research questions to ensure focused and structured interpretation. The qualitative data that was gathered from 15 industry experts during the data collection is explained in the above analysis chapter according to the codes they were classified into. This chapter focuses on discussing the relevant findings in relation to the research questions and objectives and the conclusion based on the findings. The discussion revolves around the three research questions and additional ones classified under "Future Perspectives" dealing with the role ISO 27001

plays, its enactment in various regions, its challenges and benefits, and how organizations can use it to ease their way through complex regulatory scenarios.

The data analysis chapter is complex due to the extensive data collection and the qualitative nature of the research method. The findings are discussed in a way that answers the main research questions. It is important to note that interviewees may not directly refer to specific regulation article numbers or ISO 27001 control numbers since participants typically do not recall the numbers by heart. However, based on the substance of the responses, the author has aligned the relevant insights with the most relevant ISO 27001 controls and legal provisions, matching them as closely as possible to the appropriate article numbers in the discussion.

5.1 RQ1- The Role of ISO 27001

What role does ISO 27001 play in organizations in meeting emerging privacy requirements?

This question was answered by several themes and codes in the data analysis. The primary theme that directly addressed this question was Theme II “Privacy Security Bridge”. Additionally, relevant insights from other themes were also considered in the process of this discussion.

The different codes under different themes answered this research question from their extracts. Particularly, the theme of the research findings, which involved "Building the Privacy Foundation" under the code "ISMS Contribution to Privacy Laws," has underscored the significance that ISO 27001 assumes for organizations that need such tools to meet new privacy requirements. As pointed out in the theoretical framework, the standard process for establishing and maintaining an Information Security Management System (ISMS) (Beckers, Heisel, Solhaug, & Stølen, 2014). ISO 27001, as an ISMS, relates to privacy laws in the main principles of confidentiality, integrity, and availability indispensable to any of the privacy regulations, such as GDPR, in terms of the scope of personal data. (See NIST,2020; Anderson,2008) Participants stressed that encryption, access control, and hashing are core aspects of confidentiality and integrity that are critical to privacy protection. This reflects ISO 27001 clause A,10 (Cryptography) and A.9 (Access Control). These controls with integration illustrate how ISO 27001 operationalize the foundational CIA principles, which are central to

all privacy regulations (GDPR Art. 32; PIPL Art. 26). This can relate to the emergence theory (Holland, 1992) by showing how privacy compliance emerges from a complex interaction between technical safeguards and security needs.

As explained in ISO/IEC 27001:2022, participants emphasized that the risk-based approach under ISO 27001 leads to early identification and timely mitigation of risks associated with personal data, which is considered a key component in the privacy compliance setup (See ISO/IEC 27001:2022, Clause 4-10). However, many participants pointed out that although ISO 27001 provides a significant foundation, it must be supplemented by privacy-specific governance measures so that it can best be applied in privacy regulations, such as lawful processing and rights of data subjects. Thus, while ISO 27001 makes a substantial contribution to privacy laws, the development of privacy-specific further controls is required for compliance.

The discussion drawn under the code "How Privacy is Built" presents a range of ways whereby organizations could infuse privacy into their very being toward the successful implementation of privacy frameworks like ISO 27001. Anticipatory governance, which is when privacy concerns are proactively handled before they escalate, is best illustrated by the implementation of centralized privacy monitoring in conjunction with dispersed accountability (Guston, 2010). In ISO 27001 Clauses 6.1 (risk assessment) and 9.3 (management review), proactive methods of detecting weaknesses inside an organization are encouraged. In line with Poli's (2017) concept of institutional foresight, a system of recursive learning is promoted by integrating training, audits, and oversight into every level of the organization.

With such a structure, it would be possible to achieve a uniform corporate governance of privacy framework along with room for business units to have sufficient flexibility in operational requirements. Further, a strong privacy culture entails compliance efforts, continuous improvement, training, and monitoring mechanisms. These play an important role in bridging privacy governance with organizational culture at multiple levels through targeted training and controls. With a management-supported approach to identifying gaps in privacy and compliance risk remediation, organizations ensure that the effectiveness of their privacy practice will meet emerging privacy regulations.

From a theoretical standpoint, the concept of emergence is reflected by the way ISO 27001 supports privacy implementation, where privacy frameworks evolve through the diverse regulatory, social and technical actors (Holland, 1992; Miller & Poli, 2010). ISO 27001 acts as an adaptable instrument that provides structure within dynamic legal environments, as well as new obligations (Article 32 or PIPL Article 55) that emerge from these inter-system interactions.

The experts further showed how structured security controls and risk-based governance of ISMS make privacy compliance a reality. Participants noted that ISO 27001 helps organizations build a strong security posture through the CIA structure, which includes confidentiality, integrity, and availability (See NIST, 2020; Anderson, 2008; Garfinkel et al., 2007; Shannon, 1949). Organizations are guided by the above-mentioned principle in integration with privacy laws. Even though ISO 27001 indicates that organizations are designating appropriate legislation and implementing security controls like encryption, access management, and risk assessments, it does not deal with privacy-specific obligations, including lawful processing, data subject rights, and privacy impact assessments. This shows that ISO 27001 is not a standalone privacy solution. However, ISO 27001 has a critical role as a privacy compliance enabler. Findings indicated that ISO 27001 certification reveals that an organization is committed to security, and therefore, it increases the possibility of passing audits and working with third parties or buyers where it is needed to show commitment to security.

Further, as per risk-based governance in ISO 27001, the clause 6.1 and clause 8.2 embodies anticipatory governance by encouraging organizations to not only respond to existing threats but also prepare for future regulatory and technological risks (Guston, 2010; Poli, 2017). This strategic foresight is aligned with GDPR Article 25(2) that emphasizes data protection by default and ongoing risk management.

The ISO 27001 standard is significant in assisting organizations in complying with newly emerging privacy requirements by integrating the relevant concepts of confidentiality, integrity, and availability to both security and privacy. The findings indicated that integrity is not only a requirement for security but also a necessity for privacy. Failure to maintain the integrity of data may lead to violations of the relevant privacy provisions. The entwined nature of ISMS (ISO 27001) and PIMS (ISO 27701) ensures that privacy is taken a deeper dimension

into security governance through the concepts of accountability, risk management, and continuous improvement. Findings indicated that the ISO 27001 standard provides a strong security foundation, but it must include additional controls representing privacy. This shows that emerging regulations can be volatile with the development of new technologies such as multi-model AI and AI governance. By ensuring that privacy and security frameworks merge rather than operate in silos, organizations can strengthen their compliance posture and build a more resilient privacy program.

Additionally, this signaling mechanism entails participants' realization of AI-related vulnerabilities and changes in priority of enforcement represents weak signals—early indicators of future regulatory transformation (Ansoff, 1985; Hiltunen, 2010). Organizations that reflect such signals in Clause 8.2 (risk assessment) and Clause 10.2 (continual improvement) must be considered forward-thinking with respect to compliance.

5.2 RQ2 – Regional Privacy Regulations

How does the implementation of ISO 27001 support compliance with emerging global privacy regulations across different regions?

This question was answered by several themes in the data analysis. The primary theme that directly addressed this question was Theme V "Tailoring the compliance suit". Additionally, relevant insights from other themes were also considered in the process of this discussion.

The introduction of ISO 27001 provides a much-needed understanding of various relationships that an organization should implement in compliance with the different global privacy regulations across regions. However, significant customization is required to fully align with diverse legal requirements. As discussed by several interviewed participants, different privacy regulations, such as GDPR, CCPA, and PIPLs in China, approach data protection differently, thus warranting different compliance strategies depending on their region. Several participants focused on an observation that the GDPR contains extensive rights of the subjects to data, whereas the PIPL of China has rights to access and rectification in a more limited sense, thereby proving that the comprehensive approach does not work in a jurisdictional base approach.

Similarly, findings indicated that while security controls were provided in ISO 27001, privacy guidance was lacking, necessitating the addition of alternative privacy assessments to the standard by organizations. This idea was further reinforced by more experts, who stated that ISMS provides the surety of privacy compliance but acts as a base with the need to include legal reviews, risk assessments, and governance mechanisms to meet every jurisdiction's specific privacy requirement.

Moreover, even though it was not in the scope of this thesis, experts elaborated on how global privacy laws are changing since most countries, Japan including South Korea, Brazil, India, and Argentina, have brought their laws demarcated along GDPR lines so that it is easy for any company fully compliant with GDPR to transition into such laws. However, problems will still be experienced in regions with rigid data localization requirements, such as China, privacy laws that compel companies to either store or process data within the boundaries of the state, imposing further compliance burden, which is not covered in ISO 27001. They are compounded further by geopolitical tensions and data transfer restrictions such as those addressed in the EU–U.S. Data Privacy Framework and the invalidation of Privacy Shield, which governed transatlantic data transfers before being struck down by the Court of Justice of the EU in 2020 (CJEU, *Schrems II*, Case C-311/18). This highlights how crucial anticipatory governance is when modifying ISO 27001 to ensure regional compliance. Participants stressed that signals such as localization requests or trends in AI enforcement need early and proper observation and planning. ISO 27001 indeed creates a solid basis for security; hence, compliance with emerging privacy laws will involve organizations remaining flexible to changes within regulations, which may require dealing with new ones in proactive terms and embedding privacy controls within the overall compliance structures.

The findings highlight that while ISO 27001 provides organizations with a structured approach to information security management, it does not inherently fulfil all privacy compliance obligations on its own. In fact, the very implementation of the standard must be appended by regulatory overlays and complemented by context to be aligned with differing privacy laws worldwide- the GDPR in Europe, CCPA in the US, and PIPL in China. As gleaned from subject matter experts, it is becoming apparent that organizations are using ISO 27001 to build into security controls their efforts at addressing privacy risks that have incorporated encryption, access management and risk assessment into their compliance efforts. However, variations in national privacy laws tend to require additional legal, contractual, and governance measures

beyond ISO 27001 to achieve overall regulatory compliance. Further research highlights similar concerns, showing that technical safeguards alone are insufficient without legal and contextual governance (Shabani & Marelli, 2019). The interview data confirms that practitioner's sense *weak signals*—e.g., stricter localization in China (PIPL Art. 38), AI-based privacy enforcement, or cross-border transfer challenges under evolving adequacy standards. Codifying such insights into Clause 6.1 (risk planning) allows ISO 27001 to become a forward-looking compliance framework. Further, this reflects anticipatory governance (Guston, 2010) by encouraging proactive adaptation to regulatory change and aligns with emergence theory (Holland, 1992) as compliance evolves from the interaction between weak signals and organizational response mechanisms (Hiltunen, 2010).

In addition, findings indicate a requirement for local and regional adaptation and localization for ISO 27001 implementation in different jurisdictions. The layers of overlays discussed among the participants show that each country has a unique interpretation and complementing requirements for compliance with privacy, even with general frameworks like GDPR. One example is the difference between the two countries, Germany and France, in terms of employee monitoring laws with Article 88 of the GDPR or stricter measures on the localization of data in China under PIPL. These show that although ISO 27001 provides a very strong security foundation, compliance strategies need to be tailored to fit such regulations. Gap analysis further underpins that fact, as ISO 27001 encompasses all data for its security and does not address privacy concerns particularly; therefore, more governance mechanisms such as privacy impact assessments, third-party risk management, and legal safeguards will be required. (Clause 6.1 – Actions to address risks and opportunities; Clause 9.1 – Monitoring, measurement, analysis and evaluation; Clause A.18.1 – Compliance with legal and contractual requirements in ISO/IEC 27001:2022**).**

These legal safeguards may include BCR (Binding Corporate Rules), SSC (Standard Contractual Clauses) for international data transfers and DPAs (Data Processing Agreements) to define responsibilities between a controller and a processor. The adaptation of ISO 27001, thus, facilitates global privacy and compliance into a solid security framework, although refinements will continuously be made to align with increasingly evolving and jurisdiction-specific compliance requirements.

Instead of a linear or uniform compliance model, the interplay of geopolitical, legal, and institutional forces gives rise to varied but interlinked privacy ecosystems (Meehl & Sellars, 1956; Miller & Poli, 2010). This mirrors the emergence theory, which states that regional customization of ISO 27001 and legal frameworks are met. ISO 27001's structural flexibility through clause 4,3 (Scope) and A.18.1.1 (applicable legislation) allows for an operational alignment in diverse jurisdictions.

As explained in the Chapter 3 theoretical framework, anticipatory governance enables organizations to anticipate future regulatory changes through foresight and strategic planning in their compliance framework **(**Guston, 2010; Poli, 2017). Weak signals provide early indicators of potential risks and shifts that may come in the future, supporting organizations in adapting their compliance efforts not only for current regulations but also for future challenges in privacy compliance (Hiltunen, 2010). In doing so, the ISO 27001 series serve as a foundation for continuous risk management and the development of flexible privacy programs that are responsive to the emerging regulatory landscape (ISO/IEC 27001:2022).
Furthermore, fostering anticipatory governance, Clause 9.2 "Internal audit" and Clause 9.3 "Management review" allow organizations to institute foresight into compliance. Internal audits could be adapted to scan for weak signals, emerging AI regulations-whereas management reviews could provide the leadership with a venue in which to discuss the adaptation of ISMS controls to the advent of future risks (Guston, 2010; Hiltunen, 2010; Poli, 2017). Thus, ISO 27001 is transformed into a future-oriented tool and not simply a static tick box.

The following table is a comparison of three privacy laws that were within the scope of the thesis: GDPR, CCPA, and PIPL. This demonstrates how ISO 27001 is relevant to global privacy regulations as it compares international privacy laws and the unique requirements of each, such as data subject rights, legal basis for processing, data localization, security measures, and enforcement. The table further covers how these areas point to the direction of compliance in various areas of application for ISO 27001 while at the same time identifying areas that require strengthening of the law, like privacy impact assessments and data protection mechanisms, to be fully compliant.

Below Table 5 shows comparison of the GDPR, CCPA, and PIPL based on the findings from the data analysis and the theoretical framework on the comparison of these privacy regulations and frameworks and how it applies to ISO 27001.

Table 5: Comparative Overview of GDPR, CCPA, and PIPL in Relation to ISO 27001 – Insights from Data Analysis and Theoretical Framework

Aspect	**GDPR (General Data Protection Regulation)**	**CCPA (California Consumer Privacy Act)**	**PIPL (Personal Information Protection Law)**
Jurisdiction	EU/EEA	California, USA	China
Scope	Applies to organizations processing personal data	Applies to, for profit entities processing personal data of Californian residents	Applies to organizations processing personal data of Chinese individuals including those outside China offering services to them
Data Subject Rights	Extensive rights including access, rectification, erasure, portability and objection.	Rights to access, delete and opt out if sake of personal information	Rights include access, rectification, erasure and portability but in a limited scope than GDPR.
Consent	Explicit, informed, freely given	Implied by default; opt-out for data sale	Prior, specific consent required for most processing
Legal Basis	Multiple (consent, contract, legal obligation)	Business purpose—no clear legal basis structure	Consent is the default; other limited lawful grounds
Data Localization	No specific requirement for data localization but	No explicit requirement for data localization	Requires localization of data for certain

	transfers outside the EU are restricted under GDPR		types of personal information
Security Measures	**Article 32** – Security of processing: Requires appropriate technical and organizational measures	Not explicitly detailed, but implied under **1798.100(e)** and **1798.150(a)(1)** requiring "reasonable security procedure	**Articles 51–56**: Require data handlers to take necessary technical and organizational measures to ensure security
Enforcement	Enforced by national data protection authorities and the European Data Protection Board (EDPB)	Enforced by the California Attorney General and private rights of action	Enforced by China's Cyberspace Administration (CAC)
Privacy Impact Assessment	Required under GDPR for high-risk processing	No explicit requirement for privacy impact assessments but mostly conduct risk assessments	Privacy impact assessments require for high-risk processing activities
Gap in ISO 27001 for compliance	ISO 27001 does not specifically address privacy concerns requiring additional legal reviews, risk assessments and	ISO 27001 provides security controls but lacks privacy specific guidance and requires legal overlays for compliances	ISO 27001 supports security but requires additional governance mechanisms including third party risk management and legal safeguards
Adaptation to local Laws	Requires local interpretation and adaptation, e.g.,	Adaptation required for specific	Requires adaptation to China's data localization and

	employee monitoring in Germany and France	California requirements	stricter data transfer mechanism
Additional Measures for Compliance	Privacy Impact Assessments (PIAs)Binding Corporate Rules (BCR), Data Processing Activities (DPAs)	Like GDPR, but SCCs and DPAs also applicable for international data transfers	Like GDPR emphasis on local data protection regulatory safeguards
Emerging Global Trends	Many Countries adopting GDPR like laws, facilitating easier compliance transitions		

This table demonstrates how ISO 27001 aligns with each of these global privacy regulations and highlights the areas where organizations must adapt or strengthen the compliance frameworks to meet jurisdiction-specific privacy laws.

5.3 RQ3 – Challenges and Benefits

What challenges and benefits do organizations face when implementing ISO 27001 for emerging privacy compliance?

5.3.1 Challenges

The findings provide an extensive overview of the challenges and advantages that organizations must face when undertaking the ISO 27001 implementation for new emerging privacy compliance, thus effectively answering Research Question 3. One of the main challenges highlighted is the resources and leadership support parameters necessary for ISO 27001 implementation. Several participants stressed that the implementation of ISO 27001 for privacy compliance becomes too burdensome without solid backing from the leadership level, including board approvals and the allocation of adequate resources. For instance, Participant 1

emphasizes the importance of obtaining management's approval of budgets and skilled personnel, while Participant 10 discusses the pitfalls of having top leadership pull support, relating to how organizations tend to engage in tokenism for the sake of compliance. This challenge evidently shows that organizational commitment is necessary to foster a culture where privacy and security are embedded in the overall business strategy.

Moreover, the dissonance between ISO 27001's focus on information security and specific privacy requirements in different regulations. Kennedy (2001) argues that legal competence tends to be limited to administrative problem-solving and, thereby, may conceal substantive legal and normative considerations. This is consistent with some criticisms levelled against technocratic legal regimes. In the case of ISO 27001, participants emphasized that on the procedural level, the standard does provide safeguards; however, the inherent processes do not address the normative privacy rights of consent or data subject rights. It appears that compliance regimes based on technological standards may not have the full place of the legal concepts unless they are made to work in tandem with others, such as ISO 27701 or some other region-specific mechanisms for privacy governance.

According to participants, the lack of specificity regarding personal data in ISO 27001 means that supplementary frameworks-such as ISO 27701-must be applied if privacy concerns are to be remedied adequately. This misalignment is accentuated by the difficulty in which organizations find themselves entrapped in aligning ISO 27001 and specific privacy regulations in various parts of the world. For instance, Participant 10 mentions issues of cross-border data transfer and compliance with domestic laws regarding the very stringent data localization rules of China. In addition, the complexity of integrating ISO 27001 with so many privacy frameworks tends to drain resources and effort, as noted by Participant 12, wasting those resources on smaller organizations that cannot keep capacity.

Organizational culture is one of the key challenges facing organizations implementing ISO 27001 in the privacy compliance dimension. An organization that does not promote a culture of security and privacy will only see the ISMS becoming ineffective. If data protection is not viewed as the responsibility of all employees, then the consistency of applying privacy best practices will suffer. The participants pointed out that compliance efforts may become sporadic or superficial in the absence of a strong internal commitment to privacy. Clause A.7.2 (Training) of ISO 27001 provides a tangible means of fostering privacy expectations

throughout the company by integrating responsibility and awareness into routine procedures. If internalization is not practised by organizations, compliance will be viewed merely as a checklist exercise detached from any meaningful interaction with privacy principles. Therefore, it remains crucial to foster shared responsibility and a continuous educational process to make a mindset that includes privacy and is not just a formal obligation. This mindset plays a broader role in the success of ISO 27001 and is influenced by media and societal narratives that shape how privacy and security are perceived within the organization. Organizational standards and social realities are shaped in large part by the media (Berger & Luckmann, 1966; Couldry, 2008). The value of security and privacy must be ingrained in the company culture, making it a shared duty. Without this attitude, putting ISO 27001 into practice could become a pointless paper exercise or a box-checking exercise without any real dedication to data protection.

Another challenge is the complexity of documentation requirements needed for ISO 27001, particularly when one considers the scope of privacy regulations. Whereas ISO 27001 lays down requirements for information security, the new privacy regulations, such as GDPR, spell out documentation requirements regarding privacy that may not touch directly on the stipulations of the standard. Organizations are often contemplating how to document the additional controls in privacy, such as DSR, breach notification, and cross-border data transfer. On top of that, documents must have some level of detail for audit purposes and yet be flexible enough to accommodate changing privacy laws, putting a burden on organizations attempting to align their security and privacy controls. Additionally, it is challenging to keep memories for foresight knowledge since these artefacts must remain adaptable to evolving privacy regulation, which can make the documentation process more complex regarding both the ISO 27001 and the emerging privacy laws (Cacciatori, 2008).

Further, many organizations have limited resources for the implementation of ISO 27001, with special reference to privacy compliance. Certification includes a serious investment of time, staff expertise, and financial resources. For smaller organizations or organizations without dedicated privacy or security teams, it becomes even more difficult. Additionally, the ISO 27001 implementation involves different elusive parties, such as the legal teams, IT, and compliance teams, who are often not good at coordination. A lack of alignment and clear communication between these departments may make the implementation of ISO 27001 more

challenging. Further, failing to completely address privacy risks can greatly impede the success of compliance activities.

Practical consideration should be effectively leveraged to utilize key controls defined in ISO27001 for responding to challenges with respect to privacy compliance, such as limitations due to lack of resources, documentation requirements, organizational culture, misalignment, and leadership support; these challenges must be aligned with privacy laws such as GDPR, CCPA, and PIPL. As discussed in Chapter 2, limited resources would be sufficiently addressed through controls like A.9.2 User Access Management or A.10 Cryptography, providing essential measures for the protection of personal data without a great deal of investment.

This misalignment also weakens the role of ISO 27001 in helping organizations prepare for future privacy risks. For example, if Clause 9.3 (management review) is only used to look back at past performance and not combined with tools that track early signs of change—like proposed laws on biometric data—then organizations miss the chance to adjust their privacy practices before new rules are enforced (Poli, 2017; Hiltunen, 2010).
To make ISO 27001 truly support anticipatory governance, Clause 10.2 (improvement) should be used not just to fix problems after they happen but to make changes in advance. This can include using foresight tools like scenario planning or monitoring weak signals—such as new trends in AI regulation—so that the organization stays ahead of legal and technological changes (Guston, 2010; Cacciatori, 2008).

By implementing secure access controls and encryption methods, organizations can ensure privacy protection in accordance with GDPR Article 32 on data security, CCPA Section 1798.150 on reasonable security practices, and PIPL Article 26 on cross-border transaction data security protections, with minimal resource allocation. A. 16 control of the ISMS (ISO27001) specifically covers the information security incidents that include documentation requirement. Further, A.18.1.4 Privacy and Protection of PII ensures that incident response procedures and privacy protections are both effectively managed and documented. Some of these critical breach reporting requirements include the provisions under articles 52-54 of the PIPL on breach reporting and other stipulations governing notifications of breach in Articles 33 and 34 of the GDPR and CCPA Section 1798.82 on breach notification requirements that demand proper documentation and communication.

Control A 7.2, Information Security Awareness and Training, helps define the organization's culture where security and privacy are set forth by the organization. GDPR Article and CCPA Section 1798.120 support this by addressing consumer rights awareness on the part of the employees. Further, Internal Organization fosters cross-departmental collaboration, addressing the issue of misalignment by clearly defining roles and responsibilities in privacy compliance is laid down under A.6.1 Internal Organization and is combed through in conjunction with the requirements of GDPR Article 24 with respect to responsibilities of the data controller, CCPA Section 1798.130 dealing with management of consumer rights, and PIPL Articles 38 and 39 on the responsibilities of data processors and controllers.

Lastly, A.5.1 Information Security Policies provides necessary leadership support by having a clear scheme that will demonstrate high management commitment, ensuring leadership role in privacy compliance as outlined by Articles 24 and 25 of the GDPR on data protection by design and by default. Section 1798.130 on consumer rights management of the CCPA; and Article 5 on principles of lawful, fair, and transparent processing of the PIPL. When strategically adapted, such controls help organizations overcome resource constraints, counter-intuitiveness of complex documentation requirements, and misalignment, improving the overall effectiveness of privacy compliance efforts.

5.3.2 Benefits

Risk management is one of the most significant benefits most organizations can derive from ISO 27001. ISO 27001 is a coherent framework for risk management, or rather a risk-based approach, for organizations to identify and respond to those risks posed by personal data processing in terms of privacy. Participants advanced that the implementation of the controls, such as multi-factor authentication (MFA), role-based access controls, and pseudonymization, has been very effective over time in attenuating the risk of personal data breaches. These controls are in line with evolving privacy laws, such as the GDPR, thus providing a strong basis for compliance and allowing for continuous management of the risks to privacy. The continual improvement principle embedded in ISO 27001 makes organizations better equipped to adjust to the times of evolving privacy regulations, thereby allowing for an approach to privacy

compliance and security that becomes more proactive. ISO 27001's Clause 6.1 and Clause 8.2 make it a highly adaptive instrument for operationalizing anticipatory governance. These clauses require organizations to identify not only known risks but also potential vulnerabilities, allowing them to build privacy capabilities aligned with future challenges—such as regulation of generative AI or cross-sector data portability (Miller et al., 2015).

Continuous improvement is another important benefit of ISO 27001. In fact, across its framework, an organization must continually assess and enhance its privacy and security controls. This uninterrupted cycle of improvement not only strengthens the overall privacy posture of the organization but also ensures the continued alignment of the organization's practices with laws and standards on privacy as they come into effect. Continuous improvement is another important benefit of ISO 27001. In fact, across its framework, an organization must continually assess and enhance its privacy and security controls. This uninterrupted cycle of improvement not only strengthens the overall privacy posture of the organization but also ensures the continued alignment of the organization's practices with laws and standards on privacy as they come into effect. According to participants, adopting a strategy like this promotes wiser choices, prevents expenses and delays, and significantly enhances security and privacy protocols. Additionally, security teams are always reviewing and improving tactics for a strong, flexible privacy-compliance system thanks to the imposed responsibility and scheduled risk reviews. Clause 10.2's emphasis on ongoing improvement by participants is consistent with anticipatory governance's focus on institutional learning and recursive foresight (Poli, 2017; Ramos, 2014). Organizations integrate resilience into their privacy plans through frequent audits and knowledge assessments (Clause 9.2).

ISO 27001 is a significant contributor to customer trust and business reputation. Many participants stressed that ISO certification serves as independent validation for an organization's commitment to data protection, easing the burden of due diligence from the shoulders of customers and partners. ISO would help organizations secure or retain customers by convincing stakeholders about the security of data management from their end according to internationally accepted norms. Given that ISO 27001 itself incorporates privacy by design to ensure that privacy goes hand in hand with security from day one, the established trust is further solidified. Hence, organizations can realize the benefits of not only enhanced internal security and privacy compliance but also greater relationships with customers who consider data protection and transparency paramount. It was illustrated that ISO 27001 certification is

becoming a trusted certification, not only because it demonstrates compliance but also because it enables businesses to demonstrate that the ISMS framework takes data security at a higher level into account. An ISO 27001 certification indicates that an organization is ready and accountable, which is increasingly of concern for the public because of data breaches or even international political crises. Even beyond its technical criteria, ISO 27001 does this by establishing credibility and confidence (Barafort, 2019).

5.4 Futures Perspectives on ISO 27001 and Privacy Compliance

The “Future Proving the Shield” theme reflects future perspectives on developing a relationship between ISO 27001, emerging technologies, and privacy regulations. In the opinion of industry experts, ISO 27001 will have to adapt to future changes in technology, especially in relation to artificial intelligence (AI) and cloud computing. Several participants pointed out that today ISO 27001 is very much focused on conventional systems and information security management. Prior to advancing on this point, they expressed the necessity of the framework to also respond to the unique threats posed by some technologies such as AI, which may involve challenges such as wrong classification of data, no "unlearning" ability of sensitive data in AI systems, and securing AI models, particularly in cloud settings. Participants suggested that AI security needs to be combined with other aspects to require a more comprehensive approach and a wider set of integrated tools dealing with privacy, cybersecurity, and AI risk management. They stressed that ISO 27001 should be sufficiently flexible to incorporate such changes soon.

The respondents from the interviews expressed concerns, saying that ISO 27001 may soon fall behind, further mentioning that new standards are beginning to emerge as privacy risks and technologies advance with age. Some experts have estimated that ISO 27001 will be absorbed completely by more recent standards or, at best, capture the expansion to incorporate additional frameworks like ISO/IEC 42001, which is the certification for Artificial Intelligence Management System Standards to address the convergence of AI, privacy, and security. Participants also stressed that soon, privacy-specific standards such as ISO 27701 (PIMS) would increasingly matter for companies particularly focused on data protection. Other experts, however, argued that excessive external framing could be misleading. The experts recommended that ISO 27001 adopt a robust stance by incorporating privacy measures into its structure, especially in areas that apply data minimization principles and data subject rights

management. According to the findings, it is important to match ISO 27001 criteria with privacy laws and other standards, especially data protection legislation like the GDPR, when it comes to management best practices. This will assist organizations in their endeavor to manage compliance within the company by identifying overlaps in requirements while avoiding duplication of efforts.

In addition to this, several participants stressed the future of ISO 27001 should rely on organizations having the capacity to revolutionize their security and privacy practices through technologies such as Privacy Enhancing Technologies (PETs) and AI efficiency-driven compliance tools. Such technological enhancements can be helpful, but careful consideration is needed to ensure human oversight to avoid errors associated with bias in AI outputs.

Additionally, the importance of awareness and education for privacy compliance was also highlighted in the discussion of future perspectives. According to experts, organizations must shift from looking at compliance merely as a financial burden to recognizing its strategic value. The stakeholders in the organization, including directors, suppliers, customers and employees, must all be made aware of the necessity of security and privacy as they cultivate a culture of best practices. When organizations consider compliance in a comprehensive manner, i.e., integrating security and privacy into the core of their operations, the organizations have greater adaptability for challenges that may arise in the future due to regulatory changes.

Hence, these findings suggest that while ISO 27001 remains a strong standard for establishing information security, its relevance will depend on the ability to adapt to fast-evolving AI, privacy, and regulatory considerations. Essentially, laying the prerequisite for the integration of privacy and security frameworks and follow-up with newly adopted technologies in an endeavor of continual education and improvement presents the best outlook for organizations in future-proofing their compliance objectives.

Emerging technology landscapes bring along new privacy risks that ISO 27001 should contend with; therefore, the ISO 27001 interview ideas will always be in step with the theoretical framework that looks at its future evolution (González, 2020). Findings indicated that that there are unique ethical threats introduced by AI technologies that the standard needs to address: data misclassification and the security of AI models themselves. This is in concert with more futures-oriented literature wherein the emphasis is on flexibility for adopting new technologies

and managing risks associated with them (Oseni et al., 2021). In addition, the integration of privacy-enhancing technologies (PET) and artificial intelligence-based tools can strengthen compliance. Hence, this should compel the adaptation and evolution of ISO 27001 in regard to these technological novelties.

Moreover, the findings indicated that the alignment of ISO 27001/27701 with privacy laws such as the GDPR, CCPA, and PIPL is necessary. It is suggested that this alignment can address the convergence of security and privacy standards, ensuring that ISO 27001 remains relevant as new regulations emerge (Hollander & Scutella, 2020). compliance is increasingly viewed as a strategic asset, and it is recommended that ISO 27001 be used to cultivate a culture in which security and privacy are intrinsically embedded within organizational processes, facilitating smooth adaptation to evolving legal frameworks. Combining this understanding with the existing literature, it is emphasized that ISO 27001 should not only accommodate advancements but also be refined in advance of what is expected in the future.

The above sheds light on the emerging challenges and opportunities for ISO 27001 in privacy compliance. The following section contains three foresight-based potential scenarios created from weak signals and interview findings. The scenarios situate ISO 27001 within potential futures as AI governance evolves, data localization becomes a stronger trend, and geopolitical fragmentation.

5.5 Scenario Projections Based on Weak Signals

A combination of these concepts presents a unified approach to operationalizing anticipatory governance and weak signal analysis in support of effective and sustained privacy frameworks. By incorporating scenario planning with clearly defined time horizons, this discussion emphasizes the need for foresight-driven decision-making to shape data protection strategies that are both resilient and adaptable (Miller & Poli, 2010; van Notten et al., 2003). The following scenario experts are grounded in empirical data derived from expert interviews and represent some of the assessed plausible directions where ISO 27001 might go between 2025 and 2035. The phrases demonstrate the lived perspectives of a few practitioners negotiating the

complexities of international privacy regulation, data localization, and the possible incorporation of AI governance within compliance frameworks.

Table 6: Practitioner Insights Informing Scenario-Based Futures for ISO 27001 (2025–2035)

Aspect	Scenario 1: Baseline – Incremental Convergence	Scenario 2: Disruption – Fragmentation and Sovereignty	Scenario 3: Transformation – Integrated Global Privacy Standard
Futures Archetype	Gradual evolution, moderate alignment	Regulatory interruption and divergence	Harmonized global standards and proactive cooperation
Role of ISO 27001	It is relevant as a foundational security tool but must be accompanied by privacy-specific tools.	Loses significance in areas with more stringent national standards or data sovereignty laws.	It receives full integration with ISO 27701 and new AI modules.
AI Regulation Impact	Slowly addressed under sector-specific or national guidance	Fragmented approaches cause incompatibility with ISO structures	The issues of AI accountability and transparency are now embedded into ISO standards that have been updated.
Data Localization Trend	Handled through SCCs, BCRs, and tailored compliance	The potent barrier with jurisdictions enacting laws that insist on local storage and review of data.	Gradually harmonized through global data governance frameworks
Compliance Strategy	Hybrid model: ISO + local legal overlays	Costly regional fragmentation; multiple governance regimes	Unified ISO-based model adopted across jurisdictions with minimal customization
ISO Adaptability	Incremental updating based on enforcement patterns and stakeholder needs.	Struggling to stay relevant while countries impose non-compatible requirements.	Actively evolving itself toward issues of privacy, AI, and ethics, effectively becoming future-ready.
Implications for Organizations	ISO helps manage complexity but is not enough alone	Greater burden of region-specific compliance, with weak global guidance	ISO becomes a one-stop solution, reducing legal complexity and enhancing trust
Insights from Interviews	"“I think ISO 27001 is helpful in the sense that it sets a good baseline. But it doesn't solve everything. For example, you still	“Even if you follow ISO, some countries don’t accept it as sufficient. You still need to store data locally or meet	“If ISO evolves to include privacy and AI, like ISO 27701 and 42001 becoming more widespread, then we could have a globally

	have to do additional work to meet GDPR.”	national security reviews.”	unified compliance approach.”

These experts have provided concrete evidence as to why futures-oriented thinking is considered an established professional practice. The Baseline scenario (scenario 1) offers ISO 27001 as a sound, stable basis in a regulatory landscape that is gradually aligning. In contrast, the Disruption scenario (scenario 2) paints a picture of growing geopolitical divergence and legal sovereignty that infringe on ISO's interoperability. Finally, the Transformation scenario (scenario 3) catches the possibility that experts increasingly dream of ISO as an integrated global standard for privacy and AI governance.Together, these insights support the use of scenario-based foresight for privacy planning and argue that the future of ISO 27001 will be shaped by the values it incorporates — particularly in how it responds to legal and technological change.

5.6 Conclusion

In conclusion, this study shows that ISO 27001 serves both as a foundation and an ever-evolving support structure for organizations seeking compliance with emerging privacy regulations such as GDPR, CCPA, and PIPL. The research findings gather both theoretical reasoning and practical insights from interviews conducted with industry professionals in multiple jurisdictions. They suggest that ISO 27001, as a structured and risk-based information security standard, won't per se cover all privacy-specific obligations. The substantive legal requirements differ on a regional basis (consider, for example, the restrictions on cross-border transfer or data subject rights), requiring organizations to impose controls beyond those of ISO 27001, including frameworks such as ISO 27701, and to recognize the interpretation of the law in the jurisdiction. Owing to its scalable and flexible nature, ISO 27001 allows organizations to foster said complementary layers without disturbing the foundation of information security management.

Moreover, the findings emphasize that ISO 27001’s value extends beyond technical security to shaping organizational governance, culture, and accountability. Its continual improvement process, outlined in Clause 10.2, promotes a dynamic compliance environment that can adapt to evolving technologies like artificial intelligence, cloud computing, and data analytics. While

challenges persist—such as implementation complexity and the gap between security and privacy—the benefits are substantial, including enhanced trust, improved risk posture, and operational efficiency. Therefore, as regulatory landscapes continue to shift and technologies introduce new ethical and legal risks, ISO 27001 must also evolve in tandem. Ongoing research, policy foresight, and integration with global privacy trends will be essential to ensuring ISO 27001 remains a future-proof foundation for privacy compliance in an increasingly complex digital world. The scenario analysis presented in Chapter 5.4.1 further strengthens this study by outlining how ISO 27001 may evolve under different future conditions, particularly in relation to AI risks, national data laws, and global standardization efforts.

5.7 Practical Implications

ISO 27001 as a strong foundation for privacy and compliance

Building a base for ISO 27001 for an organization's information security management system may ensure strong confidentiality integrity and availability of the data. This foundation should be integrated to a broader privacy compliance framework by aligning with the personal data protection regulations such as GDPR, CCPA and PIPL. More specific privacy obligations could be related to the data subject rights and lawful processing. For instance, an organization in Finland could rely on ISO 27001 as the foundation for a risk-based definition of security risks associated with personal data but also include privacy-specific governance measures such as the conduct of Privacy Impact Assessments (PIAs) and having appointed Data Protection Officers (DPOs) for effective privacy management. To ensure that an organization is compliant the GDPR lawful processing requirements under Article 6 controls such as A.9 (Access Control) and A.10 (Cryptography should be considered and applied with the aim of guaranteeing that the data is accessed securely.

Customization for Global Privacy Regulations

Organizations must consider regional laws when implementing ISO 27001.The processes should be tailored to jurisdiction-based stipulations. For instance, Data localization in China as

provided by the PIPL or string employee monitoring regulations in Germany (under the GDPR Article 88). ISO 27001's A.15 (Supplier Relationships) can help ensure compliance with PIPL cross border data transfer provisions including the requirement for a security assessment prior to data. However, this must be done cautiously as the legal interpretations of different jurisdictions may still vary with the language and the use case scenarios. To ensure that the ISMS and privacy management systems adapt well to different data protections laws and regulations, a multinational organization will regularly perform gap analyses and develop other policies and processes to the regional needs.

Integration with privacy standards

Although ISO 27001 develops a prudent security framework, it does not however comprehensively address the privacy obligations. To properly investigate the data subject rights under the GDPR, ISO 27701 can be integrated with ISO 27001, using controls like A.7.2 (Information Security Awareness and Training) to ensure that employees are aware of the data subject rights and comply with GDPR requirements such as access, rectification and data portability (Article 15-20 of GDPR). For instance, organizations may need to consider ISO 27701 (PIMS) to achieve an advanced level of privacy compliance, especially in the areas of rights of the data subject and processing activities. This could enhance the overall capability of the organization's requirement of the privacy and security efforts.

Continuous Improvement and Adaptability to emerging trends

Continuous Improvement is one of the main principles that came across in this study especially from the industry experts. Continual improvement in ISO 27001 involves the proactive identification of opportunities to enhance security controls, improve compliance with policies and standards, and respond to changes in the threat landscape and business environment (ISO/IEC 27001:2022, Clause 10.2). Organization remains flexible to evolving environment concerning new privacy regulations and emerging risk such as threats and opportunities from AI. As AI progresses organizations have to transition their current workflow and organizational culture into a more AI friendly culture to utilize the organizational resources more efficiently. However, due to the biasness or potential threats that AI algorithms can cause regular reviews if privacy impact assessments need to be carried out and Privacy Enhancing Technologies (PETs) should be adapted.

Leadership and Resource Allocation

Privacy can create an environment where all employees in all functions become champions of compliance with ISO 27001. The company should also appoint a senior privacy officer and or a chief information security officer (CISO) to oversee the execution of ISO 27001 within the company that is based in the location of the organization where implementation is closely aligned with the regulations. To ensure compliance with GDPR's requirement, which is accountability under Article 5(2), appointing a senior privacy officer or CUSO can support monitoring an enforcing the privacy and security policies at organizational level. Regular training aimed at improving privacy knowledge and skills, therefore, will help the company reach greater compliance preparedness.

Embedding a Cross-Organizational Culture of Privacy and Security

It is important for organizations to develop a culture of finding privacy and security as joint responsibilities of every employee as opposed to specialized departments. Such culture change can have delivery methods such as awareness programs, training, and incentive schemes for best practices. Such participation could include annual programs on privacy and security awareness for employees in a global company to strengthen in them the message of importance for protecting data and compliance with the applicable privacy laws. In addition, making it clear to all departments (like HR, IT or marketing, etc.) what is required from them in maintaining the privacy standards would be a big boost in improving compliance results. The training outlined in A.7.2 (Information Security Awareness and Training) can be expanded to include awareness of both privacy and security best practices, directly aligning with Article 25 of GDPR, which mandates "Data Protection by Design and by Default."

Ongoing Legal Monitoring and Gap Analysis

Organizations should always track the progress of changes in privacy laws through organizations while conducting periodic gap assessments in its implementation of ISO 27001 standards to satisfy new regulatory demands and spate of latest threats. For instance, an organization could set up a quarterly review mechanism for changes in privacy regulations across regions (e.g. Updates to the CCPA, Brazil's LGPD) and determine changes to its privacy governance framework as per these findings. To stay compliant with evolving privacy laws

such as the CCP, organizations should utilize ISO 27001's A.18.1.4 (Privacy and Protection of PII), conducting quarterly reviews and updates to their privacy governance framework in line with regulatory developments.

5.8 Validity of the research

This study's validity through a systematic qualitative research design grounded in empirical evidence collected from 15 industry experts across multiple regions and multiple industries where the size was ranging from 10 billion turnover to 1 billion turnover (USD). Further, it is important to note that the majority of the companies where the participants worked were B2B corporations. Testing a traditional hypothesis was not considered in this thesis; rather, an exploratory approach was used, using thematic analysis to generate insights from industry experts. The NVivo software supported transparency and consistency in the coding process when analyzing a comprehensive data collection across 15 industry experts.

The dependability was addressed by a six-phase process of thematic analysis by Braun Clarke (2022). This is a qualitative nature prioritized study and the depth, and the contextual understanding was prioritized over generalizability, Further the technical information such as the legislature article numbers and ISO 27001 controls were used all throughout the study to maintain the required level of standard that is expected by this study. This study could be highly valuable for industry-based information security and privacy experts as the research questions are applicable to every industry that is struggling to be compliant and maintain information security simultaneously. Although limitations of the study have been addressed separately, the transparency in method, reflexivity, and rich expert data contribute to the trustworthiness and confirmability of the findings.

5.9 Suggestions for Futures Research

As suggestions for future research, a comparative analysis of ISO 27001 and other international standards, such as the NIST Cybersecurity Framework (NIST CSF) and SOC 2, especially in how they address privacy and security integration in different jurisdictions, can be conducted. The literature would be enriched by a deeper inquiry into how organizations leverage these frameworks in parallel or selectively based on their regulatory environment and business

models (e.g., B2B vs B2C). Practical insights for organizations to develop integrated compliance strategies can be provided by exploring the relationship between ISO 27001 and ISO 27701 (Privacy Information Management), as well as emerging standards like ISO 31700 (Privacy by Design for Consumer Goods). By focusing on how these standards adapt to risks related to algorithmic transparency, data sovereignty, and ethical AI use under new and evolving regulations, future studies could benefit, given the relevance of AI governance.

Further research in this respect should consider incorporating more jurisdictions such as South Africa (POPIA), Brazil (LGPD), India (Digital Personal Data Protection Act, 2023), Australia (Privacy Act amendments), and Middle Eastern countries such as the UAE and Saudi Arabia. These regions are witnessing dynamic legal reforms and throwing light on the varied local scenarios based on cultural, legal, and infrastructural settings that affect the implementation of ISO 27001. It may also be worthwhile for future research to establish a longitudinal design as it could give insights into the progress of ISO 27001 adoption as a sight for global privacy shifts and technological disruption over time. Furthermore, empirical studies involving SMEs and non-technological sectors may reveal whether the perceived strengths and weaknesses of ISO 27001 change based on the maturity of the organization, the risk exposure of the sector, or upon different layers of regulatory pressure from the region.

6. References

Ahlqvist, T. – Halonen, M. – Eerola, A. – Kivisaari, S. – Kohl, J. – Koivisto, R. – Wessberg, N. (2012) Systemic transformation, anticipatory culture, and knowledge spaces: Constructing organisational capacities in roadmapping projects at VTT Technical Research Centre of Finland. *Technology Analysis & Strategic Management*, Vol. 24 (8), 821–841.

Aguilera, R. V. – Jackson, G. (2003) The cross-national diversity of corporate governance: Dimensions and determinants. *Academy of Management Review*, Vol. 28 (3), 447–465. https://doi.org/10.5465/amr.2003.10196772

Ahlqvist, T. – Valovirta, V. – Loikkanen, T. (2012) Systemic transformation, anticipatory culture, and knowledge spaces: Constructing organisational capacities in roadmapping projects at VTT Technical Research Centre of Finland. *Futures*, Vol. 44 (10), 868–877. https://doi.org/10.1016/j.futures.2012.07.001

Alrehili, A. A. – Alhazmi, O. H. (2024) ISO/IEC 27001 Standard: Analytical and Comparative Overview. In: *Advances in Data-Driven Computing and Intelligent Systems*, 143–156. Springer Nature Singapore. https://doi.org/10.1007/978-981-99-9524-0_12

Anderson, Ross (2008) *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Wiley.

Ansoff, H. Igor (1975) Managing strategic surprise by response to weak signals. *California Management Review*, Vol. 18 (2), 21–33.

Ansoff, H. Igor (1985) *Implanting Strategic Management*. Prentice Hall.

Beckers, K. – Heisel, M. – Solhaug, B. – Stølen, K. (2014) ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system. In: *Engineering Secure Future Internet Services and Systems*, ed. by M. Heisel – W. Joosen – J. Lopez – F. Martinelli, 315–344. Springer. https://doi.org/10.1007/978-3-319-07452-8_13

Berger, Peter L. – Luckmann, Thomas (1966) *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Anchor Books.

Bevir, Mark (2013) *A Theory of Governance*. University of California Press.

Bhargav-Spantzel, A. – Squicciarini, A. C. – Modi, S. – Young, M. – Bertino, E. – Elliott, S. J. (2007) Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, Vol. 15 (5), 529–560. https://doi.org/10.3233/JCS-2007-15503

Bradford, Anu (2020) *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Braun, Virginia – Clarke, Victoria (2012) Thematic analysis. In: *APA Handbook of Research Methods in Psychology*, Vol. 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological, ed. by H. Cooper – P. M. Camic – D. L. Long – A. T. Panter – D. Rindskopf – K. J. Sher, 57–71. American Psychological Association. https://doi.org/10.1037/13620-004

Beckers, F. (1997) ISO 9000: Marketing motivations and benefits. *International Journal of Quality & Reliability Management*, Vol. 14 (9), 936–947. https://doi.org/10.1108/02656719710186867

Braun, Virginia – Clarke, Victoria (2024) Thematic analysis. In: *Encyclopedia of Quality of Life and Well-Being Research*, 7187–7193. Springer International Publishing, Cham.

Bughin, J. – Chui, M. – Manyika, J. (2013) Ten IT-enabled business trends for the decade ahead. *McKinsey Quarterly*, Vol. 13 (May), 1–13.

Bygrave, L. A. (2010) The place of privacy in data protection law. In: *Privacy and Data Protection: An Element of Choice*, ed. by S. Gutwirth – Y. Poullet – P. De Hert – R. Leenes, 3–13. Springer. https://doi.org/10.1007/978-94-007-0641-9_1

Cacciatori, E. (2008) Memory objects in project environments: Storing, retrieving and adapting learning in project-based firms. *Research Policy*, Vol. 37 (9), 1591–1601. https://doi.org/10.1016/j.respol.2008.06.005

California Legislature (2018) *California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 et seq. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5&part=4.&chapter=&article=

California Legislature (2020) *California Privacy Rights Act of 2020 (CPRA)*, amending Cal. Civ. Code § 1798.120. https://oag.ca.gov/privacy/ccpa

Cate, F. H. (2020) The failure of the United States to protect privacy. *International Data Privacy Law*, Vol. 10 (4), 271–281. https://doi.org/10.1093/idpl/ipaa015

Cavoukian, Ann (2011) *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers*.

Clarke, Victoria – Braun, Virginia (2016) Thematic analysis. In: *Analysing Qualitative Data in Psychology* (2nd ed.), ed. by E. Lyons – A. Coyle, 84–103. Sage.

Council of Europe (1950) *European Convention on Human Rights*. https://www.echr.coe.int/documents/convention_eng.pdf

Couldry, Nick (2008) Mediatization or mediation? Alternative understandings of the emergent space of digital storytelling. *New Media & Society*, Vol. 10 (3), 373–391. https://doi.org/10.1177/1461444808089414

Craig, Paul – De Búrca, Gráinne (2021) *EU Law: Text, Cases, and Materials* (7th ed.). Oxford University Press.

Creswell, John W. – Poth, Cheryl N. (2018) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (4th ed.). SAGE Publications.

Court of Justice of the European Union (2020) *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), Case C 311/18*, ECLI:EU:C:2020:559. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311

Denzin, Norman K. – Lincoln, Yvonna S. (2000) *Handbook of Qualitative Research* (2nd ed.). SAGE Publications, Thousand Oaks, CA.

Denzin, Norman K. – Lincoln, Yvonna S. (2005) *The SAGE Handbook of Qualitative Research* (3rd ed.). SAGE Publications, Thousand Oaks, CA.

De Haan, Henk (2006) How emergence arises. *Ecological Complexity*, Vol. 3 (4), 293–301. https://doi.org/10.1016/j.ecocom.2007.02.003

De Hert, Paul – Papakonstantinou, Vagelis (2013) Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency. *I/S: A Journal of Law and Policy*, Vol. 9 (2), 271–324.

Dufva, Mikko – Ahlqvist, Toni (2015) Knowledge creation dynamics in foresight: A knowledge typology and exploratory method to analyse foresight workshops. *Technological Forecasting and Social Change*, Vol. 94, 251–268. https://doi.org/10.1016/j.techfore.2014.10.00

European Data Protection Board (n.d.) *Tasks and Duties*. https://edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en

European Union (2000) *Charter of Fundamental Rights of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT

European Union (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Fereday, Jennifer – Muir-Cochrane, Eimear (2006) Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, Vol. 5 (1), 80–92.

Fitzgerald, Brian – Howcroft, Debra (1998) Competing dichotomies in IS research and possible strategies for resolution. In: *Proceedings of the Nineteenth International Conference on Information Systems (ICIS)*, ed. by R. Hirschheim – M. Newman – J. I. DeGross, 155–164.

Gibbson, David – Henrikson, Linda (2011) The adaptation of quality standards: A comparative study of ISO practices in the US and UK. *Journal of Management Systems*, Vol. 23 (2), 45–62.

González Fuster, Gloria (2014) *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer. https://doi.org/10.1007/978-3-319-05023-2

Grant, Cynthia – Osanloo, Azadeh (2014) Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "house." *Administrative Issues Journal: Connecting Education, Practice, and Research*, Vol. 4 (2), 12–26. https://doi.org/10.5929/2014.4.2.9

Greenleaf, Graham (2021) Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, No. 170, 1–6.

Guston, David H. (2010) Anticipatory governance of emerging technologies. *Journal of the Korean Vacuum Society*, Vol. 19 (6), 432–441.

Hevner, Alan R. – March, Salvatore T. – Park, Jinsoo (2004) Design Science in Information Systems Research. *MIS Quarterly*, Vol. 28 (1), 75–105.

Hiltunen, Elina (2010) *Weak Signals in Organizational Futures Learning* (Doctoral dissertation). Helsinki School of Economics, Aalto University.

Holland, John H. (1992) Complex adaptive systems. *Daedalus*, Vol. 121 (1), 17–30. https://www.jstor.org/stable/20025416

Holland, John H. (1992) *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence* (2nd ed.). MIT Press.

International Organization for Standardization (2018) *ISO/IEC 27000:2018 – Information Security Management Systems – Overview and Vocabulary*. ISO.

International Organization for Standardization (2022) *ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*. ISO. https://www.iso.org/standard/82875.html

Jissink, Tessa – Rohrbeck, René – Hölzle, Kathrin (2014) Corporate foresight: Antecedents and contributions to innovation performance. *Technological Forecasting and Social Change*, Vol. 101, 1–14. https://doi.org/10.1016/j.techfore.2014.08.012

Kaur, Amandeep – Kochhar, Sandeep – Ganguli, Anshu – Rajest, S. S. (2021) Evolution of management system certification: An overview. In: *Handbook of Research on Future Opportunities for Technology Management Education*, 1–24. IGI Global.

Kaushik, Vikas – Walsh, Christine A. (2019) Pragmatism as a research paradigm and its implications for social work research. *Social Sciences*, Vol. 8 (9), 255. https://doi.org/10.3390/socsci8090255

Kennedy, David (2001) The role of law in economic thought: Essays on the fetishism of commodities. *The American University International Law Review*, Vol. 19 (1), 101–137.

Konvitz, Milton R. (1966) *Privacy and the Law: A Philosophical and Constitutional Inquiry*. Columbia University Press.

Kvale, Steinar – Brinkmann, Svend (2009) *InterViews: Learning the Craft of Qualitative Research Interviewing* (2nd ed.). SAGE Publications, Thousand Oaks, CA.

Lesca, Hubert – Lesca, Nicolas (2014) *Weak Signals for Strategic Intelligence: Anticipation Tool for Managers*. Wiley-ISTE.

Lincoln, Yvonna S. – Guba, Egon G. (1994) Competing paradigms in qualitative research. In: *Handbook of Qualitative Research*, ed. by N. K. Denzin – Y. S. Lincoln, 105–117. SAGE Publications, Thousand Oaks, CA.

Liu, Han – Lin, Dan (2022) Data localization and cross-border data transfer in China: PIPL and beyond. *Computer Law & Security Review*, Vol. 45, 105700. https://doi.org/10.1016/j.clsr.2022.105700

Liu, L. – Chen, Y. (2024) A triple-layered comparative approach to understanding new privacy policy practices of digital platforms and users in China after implementation of the PIPL. *Social Media + Society*, Vol. 10 (4), 20563051241301265. https://doi.org/10.1177/20563051241301265

Meehl, Paul E. – Sellars, Wilfrid (1956) The concept of emergence. *Minnesota Studies in the Philosophy of Science*, Vol. 1, 239–252.

Miller, Riel (2018) *Transforming the Future: Anticipation in the 21st Century*. Routledge.

Miller, Riel – Poli, Roberto – Rossel, Pierre (eds.) (2015) *Anticipatory Governance: Practical Approaches to Dealing with the Future*. UNESCO Chair in Anticipatory Systems.

Miller, Riel – Poli, Roberto (eds.) (2010) *Anticipatory Systems and the Philosophical Foundations of Futures Studies* [Special issue]. *Foresight*, Vol. 12 (3).

Miller, Riel – Poli, Roberto (2010) Anticipatory systems and futures studies. In: *Handbook of Anticipation: Theoretical and Applied Aspects of the Use of Future in Decision Making*, ed. by R. Poli. Springer.

Monev, V. (2020). Organisational information security maturity assessment based on ISO 27001 and ISO 27002. In *2020 International Conference on Information Technologies (InfoTech)* (pp. 1–5). IEEE.

National Institute of Standards and Technology (2017) *An Introduction to Information Security (NIST Special Publication 800-12 Rev. 1)*. https://doi.org/10.6028/NIST.SP.800-12r1

OECD (2009) *OECD Health Data 2009*. OECD. http://www.ecosante.org/index2.php?base=OCDE&langh=ENG&langs=ENG, retrieved 9.9.2009.

Oseni, Abubakar – Moustafa, Nour – Janicke, Helge – Liu, Peng – Tari, Zahir – Vasilakos, Athanasios (2021) Security and privacy for artificial intelligence: Opportunities and challenges. *arXiv preprint arXiv:2102.04661*. https://arxiv.org/abs/2102.04661

Peltier, Thomas R. (2016) *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.

Pezzulo, Giovanni – Rigoli, Francesco (2011) The value of foresight: How prospection affects decision-making. *Frontiers in Neuroscience*, Vol. 5, Article 79. https://doi.org/10.3389/fnins.2011.00079

Poli, Roberto (2017) *Introduction to Anticipation Studies*. Springer.

Qusef, Abdallah – Alkilani, Hamzeh (2022) The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Computer Science*, Vol. 8, e810.

Ramos, Jose M. (2014) Anticipatory governance: Traditions and trajectories for strategic design. *Journal of Futures Studies*, Vol. 19 (1), 35–52. https://doi.org/10.6531/JFS.2014.19(1).A35

Rhodes, R. A. W. (1997) *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*. Open University Press.

Richards, Neil M. (2013) The dangers of surveillance. *Harvard Law Review*, Vol. 126 (7), 1934–1965.

Rohrbeck, René (2012) Exploring value creation from corporate-foresight activities. *Futures*, Vol. 44 (5), 440–452. https://doi.org/10.1016/j.futures.2012.03.006

Schwartz, Paul M. – Solove, Daniel J. (2021) The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review*, Vol. 86 (6), 1814–1894.

Shabani, Mahsa – Marelli, Luca (2019) Re-identifiability of genomic data and the GDPR. *EMBO Reports*, Vol. 20 (6), e48316. https://doi.org/10.15252/embr.201948316

Shaffer, Gregory C. – Pollack, Mark A. (2004) Hard and soft law in international governance. In: *Transnational Governance and Constitutionalism*, ed. by C. Joerges – J. Sand – G. Teubner, 197–218. Oxford University Press.

Shannon, Claude E. (1949) Communication theory of secrecy systems. *The Bell System Technical Journal*, Vol. 28 (4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Solove, Daniel J. (2004) *The Digital Person: Technology and Privacy in the Information Age*. New York University Press.

Solove, Daniel J. – Schwartz, Paul M. (2020) *Information Privacy Law* (6th ed.). Wolters Kluwer.

Standing Committee of the National People's Congress (2021) *Personal Information Protection Law of the People's Republic of China (PIPL)*. Effective November 1, 2021. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Stoker, Gerry (1998) Governance as theory: Five propositions. *International Social Science Journal*, Vol. 50 (155), 17–28. https://doi.org/10.1111/1468-2451.00106

Szabó, Máté Dániel (2005) On the differences between EU and US privacy protection. In: *Evolution of Concepts of Privacy and Personal Data Protection under the Influence of Information Technology Development*, 47–60. Global Research Publishing.

Thomas, David R. (2006) A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, Vol. 27 (2), 237–246. https://doi.org/10.1177/1098214005283748

Tikkinen-Piri, Christina – Rohunen, Anni – Markkula, Jouni (2018) EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, Vol. 34 (1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

United Nations (1948) *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations (1966) *International Covenant on Civil and Political Rights*. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

van Notten, Philip W. F. – Rotmans, Jan – van Asselt, Marjolein B. A. – Rothman, Dale S. (2003) An updated scenario typology. *Futures*, Vol. 35 (5), 425–443.

Wang, Fangfang (2021) China's Personal Information Protection Law: What businesses need to know. *International Data Privacy Law*, Vol. 11 (3), 220–230. https://doi.org/10.1093/idpl/ipab011

Whalen v. Roe, 429 U.S. 589 (1977).

White, David – Fortune, Joyce (2002) Current practice in project management—An empirical study. *International Journal of Project Management*, Vol. 20 (1), 1–11. https://doi.org/10.1016/S0263-7863(00)00029-6

Wiander, Tuomas (2007) Positive and negative findings of the ISO/IEC 17799 framework.

This thesis cites ISO/IEC 27001:2022 for academic purposes. No proprietary or non-public content from ISO materials has been reproduced. All references are based on publicly available information and secondary academic sources.

Appendices

Appendix 1: Interview Questions

The Role of ISO 27001 in Emerging Global Privacy Frameworks (GDPR, CCPA, and PIPL) **Interview Questionnaire**

PART I: Background & Setting the Context

1. Could you briefly explain your role in your organization and your responsibilities related to privacy compliance or information security?
2. How many years of experience do you have working with ISO 27001, privacy compliance, or related frameworks?
3. Can you share your understanding of ISO 27001 and its relevance to privacy compliance?
4. Has your organization's approach to privacy compliance evolved over time? If yes, how?

PART II: Role of ISO 27001 in Emerging Privacy Requirements
(Addressing Research Question 1: What role does ISO 27001 play in organizations in meeting emerging privacy requirements?)

1. How does your organization perceive the role of ISO 27001 in meeting emerging privacy requirements?
2. In your experience, how might ISO 27001 contribute to addressing future privacy laws or anticipated regulatory changes?
3. Are there specific privacy requirements (e.g., data subject rights, data minimization) where you expect ISO 27001 to play an increasingly prominent role?
4. In your opinion, should ISO 27001 evolve to better address anticipated privacy trends? If yes, how?

PART III: Supporting Global Privacy Compliance Across Regions
(Addressing Research Question 2: How does the implementation of ISO 27001 support compliance with global privacy regulations across different regions?)

1. Do you think ISO 27001 will continue to facilitate compliance with regulations such as GDPR, CCPA, and China’s PIPL, especially as these laws evolve?
2. Are there expected regional developments or future privacy standards that may impact how ISO 27001 is applied?
3. How might your organization address future gaps between ISO 27001 and emerging regional privacy requirements?
4. Do you think ISO 27001’s global standardization will be sufficient to adapt to rapidly evolving privacy regulations in the coming years?

PART IV: Challenges and Benefits of ISO 27001 in Emerging Privacy Compliance (Addressing Research Question 3: What challenges and benefits do organizations face when implementing ISO 27001 for emerging privacy compliance?)

1. What anticipated challenges will your organization faced during ISO 27001 implementation related to privacy compliance?
2. Are there future-focused capabilities or strategic resources that will become increasingly critical to successful implementation?
3. What benefits have you observed from using ISO 27001 for privacy compliance (e.g., improved data governance, risk management)?
4. How does ISO 27001 shape your organization's decision-making around privacy compliance?
5. Are there specific instances where ISO 27001 provided measurable outcomes for privacy compliance?

PART V: Future Perspectives on ISO 27001 and Privacy Compliance

1. Based on your experience, how do you see the role of ISO 27001 evolving in light of emerging privacy frameworks globally?
2. Are there any emerging trends or best practices that organizations should consider when leveraging ISO 27001 for privacy compliance?
3. What advice would you give to organizations aiming to align ISO 27001 with future anticipated privacy requirements?

Thank you for your participation in this study. Your contribution is invaluable to advancing research in privacy compliance and information security.

Appendix 2: Interview Invitation

Interview Questionnaire

"ISO 27001 and Global Privacy Compliance
The Role of ISO 27001 in Emerging Privacy Frameworks in Europe, the USA and China"

Dear Recipient,
Thank you once again for agreeing to participate in my master's thesis research! I truly value your insights, and I want to ensure this process is comfortable and straightforward for you.
Please find the interview questions attached to this email. Here are a few things to keep in mind:

- **Answering Questions**: You are welcome to answer based on your knowledge and experience. *It's completely okay if you don't have deep expertise in every area—your perspective is still incredibly valuable*.
- **Preparation**: Feel free to review the questions beforehand and prepare your responses at your convenience.
- **Skipping Questions**: If there's any question, you're unsure about or would prefer not to answer, you can simply skip it.
- **Withdrawal**: You have the right to withdraw your contribution at any point before the final publication of my thesis, no questions asked.

Anonymity: Your identity and responses will be fully anonymized in my research. No personal or organizational details will be shared.

If you have any questions, concerns, or need clarification about any of the topics, please don't hesitate to reach out.

Thank you for contributing to my research! I truly appreciate your time and support.

Best regards,
Asanka Ishari Wedeha Pathirana
Master's Student at University of Turku

Appendix 3: Research Data Privacy Notice

Data Privacy Notice for Research Participants

You are invited to participate in a research study titled **"ISO 27001 and Global Privacy Compliance"** This study aims to explore the role of ISO 27001 in addressing compliance with global privacy regulations. Your participation is voluntary and involves responding to interview questions. You may withdraw at any time without any negative consequences.

This notice provides detailed information about how your personal data will be collected, processed, and protected in compliance with the EU General Data Protection Regulation (GDPR), and other relevant data protection laws.

1. **Name of the Register**

"ISO 27001 and Global Privacy Compliance
The Role of ISO 27001 in Emerging Privacy Frameworks in Europe, the USA and China"

2. Data Controller
Name: Asanka Ishari Wedeha Pathirana
Position: (disclosed)
Company: (disclosed)
Institution: University of Turku
Contact Information:
Email: (disclosed)
Phone: (disclosed)

3. Purpose and Legal Basis for Processing Personal Data
The purpose of this study is to gather insights from privacy and information security experts on ISO 27001 and its application in global privacy frameworks, including GDPR, CCPA, and PIPL.
The legal basis for processing your personal data is:

- **Consent:** Your explicit consent to participate in the study (GDPR Article 6(1)(a)).
- **Scientific Research:** Processing is necessary for scientific research purposes (GDPR Article 6(1)(e)).

4. Types of Personal Data Processed
The following personal data may be collected and processed:

- Name and email address (for communication purposes).
- Profession and years of professional experience.
- Recorded voice data (from interviews).
- Interview transcripts (anonymized for analysis).

5. Recipients of Personal Data
Your personal data will be handled solely by the researcher and will not be shared with third parties. Anonymized data, which no longer qualifies as personal data, may be retained for further academic research or publications.

6. Transfer of Data to Third Countries
No personal data will be transferred outside the EU/EEA. Any collaboration with researchers or institutions in third countries will involve only anonymized data, ensuring compliance with GDPR and other applicable laws.

7. Retention Period of Personal Data
- Recorded interviews will be stored securely for a maximum of two years.
- After transcription, only anonymized data will be retained for further academic purposes.
- Personal data will be permanently deleted upon completion of the study or earlier if requested by you.

8. Rights of the Data Subject
As a research participant, you have the following rights under GDPR:
- **Right to Information:** To be informed about how your data is processed.
- **Right of Access:** To request a copy of your personal data.
- **Right to Rectification:** To correct any inaccuracies in your data.
- **Right to Restrict Processing:** To request limited processing of your data under certain conditions.
- **Right to Object:** To object to the processing of your personal data.
- **Right to Erasure (Right to be Forgotten):** To request deletion of your data unless retaining it is necessary for scientific research or public interest purposes.

To exercise these rights, please contact the Data Controller using the information provided in Section 2.

9. Automated Decision-Making and Profiling
Your data will not be used for automated decision-making or profiling.

10. Anonymization and Data Security Measures
All personal identifiers will be removed during transcription to ensure anonymity. Data will be stored on encrypted devices and protected with secure access controls. Only anonymized data will be used for analysis and reporting.

11. Further Information

If you have any questions about the study or your data protection rights, please contact:
Asanka Ishari Wedeha Pathirana
Email (disclosed)
Phone Number (disclosed)

Thank you for your participation in this study. Your contribution is invaluable to advancing research in privacy compliance and information security.
Asanka Ishari Wedeha Pathirana

Appendix 4: Interview Transcript Extracts

To protect the confidentiality and privacy of the interview participants and their organizations, the interview extracts included in this thesis have been carefully edited. Personal identifiers and sensitive organizational details have been modified or anonymized to ensure that no individual or entity can be recognized. These edits were made solely to safeguard confidentiality and do not alter the meaning or integrity of the responses. The content remains faithful to the participants' original insights and accurately reflects the information they provided.

Interview Extracts

Participant 8

"So, I'd say ISO 27,001 sets a higher standard than most privacy laws allow. Again, privacy laws are following one of two pathways. Now, they're all mimicking a GDPR based approach, So, what we're seeing now is obviously ISO 27,001 standards. They've not been officially recognized as being a certification scheme under GDPR, but what it is showing is, is that you're meeting these kinds of standards. The way I see is, if a company has ISO 27,001 certification, they're likely to pass a GDPR audit"

"Even if that is a most modern technique multi factor authentication you have a token in your phone or a device, and when you talk about the encryption algorithm or hashing, these are new things that came in. ex is very important to check the integrity of data. If you cannot establish the integrity of the personal data that is also a violation of privacy. In the pillar of Privacy there are confidentiality, integrity and availability and these are quite same for ISMS as well.. The ISMS is seen as a bigger bucket they go on protecting all types of data whereas privacy is protecting personal data."

"When I think if ISO, I think of cybersecurity, not privacy, ISO has tried to add privacy elements over the years, but people still confuse security with privacy. Just because you lock data behind a door doesn't mean you' ve addressed privacy. Privacy is about Human Rights, and it is deeper than cyber security. Privacy is about who has the right to access and how they use the personal data, not just about keeping it safe"

"I think probably the part where people get tripped up on ISO is that it is, is? It is a very robust framework. But not all companies do all things, so figuring out what applies to them and what doesn't instead of them. You know, some companies feel like, okay, well, this is on the list. So, we don't do this thing, but maybe we should do this thing, or maybe we should say that we do this thing. So, I think the challenge with almost any framework is for companies to be able to state what they do or what they don't do, and then not waste a lot of time trying to create the impression that they do something that they do not do."

“Privacy is about protecting individuals’ rights—not just locking data behind a door. In my experience, ISO 27001 often focuses more on operational controls than true privacy concerns. For example, one company required weekly emails to IT confirming database access reviews, but that felt more procedural than privacy-focused. Another issue is that ISO evidence can be manufactured—some companies scramble to fabricate compliance just before audits. While ISO is a helpful guide, it doesn’t fully address privacy and likely never can. It’s fundamentally different."

"The U.S. privacy landscape is extremely complex—there’s no comprehensive federal regulation, only sector-specific laws like HIPAA. But HIPAA isn't truly a privacy law; it’s about data portability and only applies within patient-provider relationships. Much personal health data falls outside its scope, which many people don’t realize. States differ too—CCPA, for example, is a complex 'layer cake' of California-specific privacy laws. In this environment, ISO can help organizations develop a data strategy—from collection to end-of-life—if it's implemented meaningfully. But if companies don't understand how to align ISO with principles like transparency, consent, and data minimization, then ISO becomes more of a lip service than a genuine privacy tool."

"ISO 27001 doesn’t fully cover privacy—it focuses more on data stewardship, like tracking how data is handled. While that’s important, companies must take further steps to address privacy meaningfully: managing data subject access requests, ensuring transparency, having a clear data collection purpose, and implementing end-of-life strategies. These granular actions go beyond what ISO can prescribe. Regulations also vary significantly—for example, only California currently allows employees to make data subject requests, adding complexity. So, while ISO offers a foundation, true privacy compliance requires proactive data governance that adapts to evolving legal landscapes."

Participant 4

“ISO 27001 has been significant in evolving privacy frameworks. It is based on the risk-based approach, and it allows organizations to identify and mitigate risks. Even though it doesn't specify what kind of data it ultimately identifies the risks for personal data as well. The continual improvements that are embedded in the standard also ensure that. For example, controls related to data encryption and access management support compliance with the GDPR.”

“So, it's not essential for a company to have to have good privacy and security practices. Obviously, it costs money to become certified. It costs money to keep the certification, but it's like me as a privacy professional having a CIPP/E OR CIPM, as a qualification. If I didn't have them, would it mean I'm less knowledgeable about privacy? No, it just a way of showing to again other people, this guy takes privacy seriously. He has a qualification in privacy. There it is. It's an easy way to show that. So that's what I see about having ISO 27001”

“I think it's helpful in the sense that it gives structure to the security controls, especially, I think, where privacy is handled by the legal department. In such cases, ISO 27001 provides confidence that security is taken seriously”

"It’s about showing a healthy respect and need for security and privacy. Resources are critical—whether it’s hiring the right people, building a privacy team, or ensuring that security

is taken seriously. The organizational culture must reflect that security and privacy are essential, not just compliance checkboxes."

“Providing documentation. So, when the assessor comes in, they will require set pieces of documentation. Now, a lot of the time with other businesses, it may be documents that they don't necessarily have, or it may be documents that they need to hastily write up. So, these, these are the issues is on. You’ll have one system set up like, like I mentioned earlier, this meeting recording on your personal device. Device, put it on a hard drive, wipe your personal device, clean it on a portable hard drive. Put them in a safe. Put that in a safe outside. Out of Mind. You and I both know that's going to meet an ISO standard because it's kept in a secure environment, limited access control, and you know it can't be copied or excavated or transferred.”

“When an ISO 27001 auditor comes in, you need to have documentation showing that you’ve done everything required. You need written evidence, all logged — what you’ve done and when you’ve done it. That’s the difficulty: a lot of companies already meet the standards, but they don’t have the evidence, and many don’t even realize they’re compliant. They focus on the cost of getting certified and think, ‘We don’t have the time or resources to commit to that right now.’

Another issue is that you don’t know what kind of assessor you’re getting. One assessor might come in with a very different standard than the next. Their thresholds for what count as a pass or fail can vary significantly. For example, in one instance, an auditor was happy just talking to me. They came in, asked about my two-year plan — what standards I aimed to achieve — not necessarily what I had already produced. They were satisfied with those answers.

But with a different assessor, that wouldn’t have been enough. They would have asked, ‘What have you delivered? Where’s the documentation? Where’s the proof?’ Some are okay if you say you’re going to do something and have it clearly planned — they’ll say, ‘We’ll come back in two years.’ But that kind of variability between auditors can be a real challenge.”

“It's easy to kind of show the paper saying we are ISO accredited. If you don't believe us, go ask ISO. Instead of saying we take privacy and security seriously, here is this stack of documents that state why we take it seriously? We could be lying. We could be trying to trick you. We could be just filling it with papers from chat GPT, but by having the actual ISO paper, you are saying, don’t believe us. Believe this credited organization who base their entire credibility, who base their entire basically, their entire business is On Being trustworthy, on providing that standard, providing that voice of reason.”

"An ISO 27001 auditor will ask how many incidents you had, but that doesn’t tell the whole story. you could have one incident, but it could be we suddenly have access to 100,000 people's financial and biometric data, or it could be one incident of somebody sending the wrong email to somebody else. Both, from a binary point of view, are a data breach. One is up here. One is negligible. ISO is more qualitative than quantitative in this regard."

"You could even see ISO itself changing—an auditor could literally just be an AI system… The potential for AI will change so many things in security and privacy, both from an administrative point of view, from a regulatory point of view, and even from a use case point of view."

“There are article many Working Party papers that indicate or strongly hint that anonymization to the GDPR standard, and obviously to other global standards, is essentially

impossible. You either anonymize it so much that any usable data from it is gone, or anonymization is being used in lieu of simply saying very high-level encryption plus pseudonymization. Anonymization has to be irreversible for a billion years, and it can't reverse that data, and essentially, that's almost impossible to prove. So, yeah, that's the other one. Is anonymization isn't possible in the way that people think it is. So that's the other technologies. If we can get full on anonymization approved by the edpb, that would also change things."

"It is about education and benefits. Going to what I said about the challenges to implementation. Lots of organizations see it as a financial burden. It is, but that burden can be offset by the benefits if you understand those benefits. So, it's about educating people as to those benefits, and if they're educated, they'll understand and hopefully start moving towards that. Best Practice, even if you get a third of the way there, then you're a third of the way ahead of many organizations who are just implementing a standard as a tick box exercise. So, education and understanding are core components, and that has to be organization wide. It has to be vertical as well as horizontal. What I mean by vertical? Educate your customers, educate your suppliers, and go across the organization. When you factor those and start considering things in the security and privacy context, then you're tending towards best practice. It starts with an idea and sharing ideas. When those ideas are shared and developed, that's where you get best practice"

"ISO 27001 reflects a commitment to respecting regulations, but not full compliance. For example, under the GDPR, ISO only addresses certain aspects—primarily security and privacy controls—not the full scope such as data subject rights, breach notification within 72 hours, or 'privacy by design' under Article 25. This limited scope is one reason why the EDPB has hesitated to authorize ISO-based certifications as demonstrating GDPR compliance. The same applies to CCPA—it may support certain controls but not reporting obligations, data subject rights, or data transfers. Under China's PIPL, ISO 27001 similarly demonstrates that an organization can secure data against external threats, but it doesn't address complex legal issues like whether a company is considered a Critical Information Infrastructure Operator (CIIO), or if data can be lawfully transferred out of China. We encountered this at XXXX where it was unclear whether our telecom operations classified us as a CIIO under Chinese law. These are issues ISO doesn't resolve. So ultimately, ISO 27001 signals an ethical or strategic commitment to better practices, not a guarantee of legal compliance."

Participant 1

"In future, ISMS right now as it is I see take care of the data protection part. With AI they will have to come up with stringiest standards. Other than simply implementing the standards or should minimize the data and only collect what they want. No matter how strict the security there is nothing 100% perfect. You end up losing the data even in strictest systems. Data minimization should be focused on. Other thing I see is that not having a proper retention policy. It is part of the ISMS too. And don't be a data holder. You must let go. Without having any feelings attached to it the data should be wiped out. Sometimes marketing folks would dig 3 years old data and try to reinvent leads. But hey the world is changing and may be those data is not even valid anymore. So, you have to put some practical thought and decide we have a robust retention policy along with a string ISMS practice."

"I know approximately around 26 controls that are important in ISO 27001 and to Privacy. My general observation is the risk or the problem you are finding in privacy has always a solution in security. If someone is unauthorized to access the data and having the access is contradictory. Access Control policy there is a solution for it and that is ISMS. That is my understanding and that is how we keep rubbing shoulders with security guys"

"That is a good question. Currently I am not seeing that, what am seeing is if someone there are 90 controls. blindly follows the 90 something controls. In 27001 ISMS and 27701 PIMS, I think most of the privacy is covered. The protection part at least. Now what remains is the core privacy, when there is a process for addressing DSR or breach notification, if you already implemented the control the risk of personal data being breached is also minimized, what we have at the moment is sufficient to address these issues."

"The most critical is the management who approves the budget. If there is no budget nothing happens. Then the human resource to take the project up. Sourcing the talent is also another thing. So, if you take care of these then the employees are the very critical part. They are also the key that security is intact, and they are also the weakest link, and breach can happen at any time."

"You must also have the sense of culture. When I say culture or compliance, doing the right thing even when nobody is watching me. That sense of belonging should be there. These are the necessary things that I believe is critical."

"What am seeing is if someone there are 90 controls. blindly follows the 90 something controls. In 27001 ISMS and 27701 PIMS, I think most of the privacy is covered. The protection part at least. Now what remains is the core privacy, when there is a process for addressing DSR or breach notification, if you already implemented the control the risk of personal data being breached is also minimized, what we have at the moment is sufficient to address these issues."

"The personal data breaches have significantly subdued over the time. The moment we decided to have a MFA in our organization a role-based access control, the moment we be serious about the classification of information and apply the pseudonymization and anonymization, the incidents have reduced."

"Whenever you are faced with an incident you have to disclose with supervisor authority and they might see you in a manner that you haven't applied these properly and then they ll have to incur some money in to credit control and what not. It is better to implement isms in order to prevent those."

"CCPA is mostly like 80% GDPR. They have copied 8-% of GDPR and made it liberal. In GDPR for an example the cookie consent, is like someone has to come and effortmetly have to say yes in order to opt it. California like you already is opted in you have to specifically opt out."

"One way to put is azure is offering you a personal tenant. There is a price model in azure cloud. They ll give you your own talent. If you implement ChatGPT or AI, it will stay there and will not be shared. So how to build security in such scenarios that ISMS must really improve."

"Under the GDPR, I'm very confident about the alignment. In the U.S., organizations tend to follow NIST under CCPA. China has its own set of regulations under the PIPL. From what I

recall, PIPL doesn't include the full set of data subject rights like GDPR or CCPA—mainly just access and rectification. So, individual rights are limited in PIPL. In terms of security, all three frameworks address protection, but PIPL is much narrower in scope. GDPR focuses heavily on confidentiality, integrity, and availability—core principles that also form the foundation of ISO 27001's Information Security Management System (ISMS). That's where the alignment lies."