

## Bachelor's Thesis

# Framework and Reference Implementation: An ISMS According to ISO/IEC 27001:2022 for SMEs in IT Security Consulting

Submitted for examination in Bachelor's degree by  
John Robert Lißke,  
904651

in the study course *Bachelor of Science IT-Sicherheit*  
at the Faculty of Informatik  
at Mobile University of Technology:  
Wilhelm Büchner Hochschule  
Hilpertstraße 31  
64295 Darmstadt

---

Supervising examiner: **CHRISTIAN HANDT**

---

Submitted: 03. May 2025

**John Robert Lißke**

**Title of thesis**

Framework and Reference Implementation:

An ISMS According to ISO/IEC 27001:2022 for SMEs in IT Security Consulting

**Keywords**

ISMS, ISO/IEC 27001:2022, SMEs, Git, GitLab, Security Compliance

**Abstract**

This thesis explores a practical solution for implementing an Information Security Management System (ISMS) in a small IT security consulting company, with the goal of developing a reference framework aligned with ISO/IEC 27001:2022. The solution addresses the unique challenges faced by small and medium-sized enterprises (SMEs), such as limited resources and lean organizational structures.

The proposed ISMS is implemented using a Git- and GitLab-based approach, enabling version-controlled documentation, transparent change tracking, and lightweight process management. Structured around the Plan-Do-Check-Act (PDCA) cycle, the system maps ISO clauses and controls to Markdown files and manages dynamic processes—such as risk management and audits—through GitLab Issues.

The thesis applies Design Science Research (DSR) to analyze the implementation and derive insights on maintainability, audit readiness, and transferability. Internal audits revealed correctable non-conformities, while the external certification audit identified no major or minor non-conformities.

The results demonstrate that a modular, Git-based ISMS is feasible, scalable, and well-suited for technically oriented SMEs aiming to achieve ISO 27001 compliance without excessive overhead.

**John Robert Lißke**

## **Thema der Arbeit**

Framework und Referenzimplementierung:

Ein ISMS gemäß ISO/IEC 27001:2022 für KMU in der IT-Sicherheitsberatung

## **Stichworte**

ISMS, ISO/IEC 27001:2022, KMU, Git, GitLab, IT-Sicherheitsmanagement

## **Kurzzusammenfassung**

Diese Bachelorarbeit untersucht eine praxisorientierte Lösung für die Umsetzung eines Information Security Management Systems (ISMS) in einem kleinen IT-Sicherheitsberatungsunternehmen. Ziel ist die Entwicklung einer Referenzimplementierung, die den Anforderungen der Norm ISO/IEC 27001:2022 entspricht und gleichzeitig den besonderen Gegebenheiten von kleinen und mittleren Unternehmen (KMU) gerecht wird.

Die Umsetzung erfolgt auf Basis von Git und GitLab, wodurch versionierte Dokumentation, nachvollziehbare Änderungen und ein schlankes Prozessmanagement ermöglicht werden. Das System orientiert sich am Plan-Do-Check-Act-(PDCA)-Zyklus und bildet ISO-Kapitel sowie Controls in Markdown-Dateien ab. Fortlaufende Prozesse wie Risikomanagement und Audits werden über GitLab-Issues gesteuert.

Im Rahmen eines Design-Science-Research-Ansatzes wird die Implementierung analysiert, um Erkenntnisse über Wartbarkeit, Auditfähigkeit und Übertragbarkeit zu gewinnen. Während interne Audits behebbare Abweichungen aufzeigten, wurden bei dem externen Zertifizierungsaudit keine Abweichungen festgestellt.

Die Ergebnisse zeigen, dass ein modulares, Git-basiertes ISMS eine praktikable und skalierbare Lösung für technisch orientierte KMU darstellt, die eine ISO-27001-Zertifizierung mit geringem organisatorischem Aufwand anstreben.

# Contents

<b>1 Introduction</b>	<b>1</b>
1.1 Problem Statement and Objectives . . . . .	1
1.2 Structure and Methodology . . . . .	2
<b>2 Theoretical Foundations: ISO/IEC 27000:2022 and ISMS</b>	<b>3</b>
2.1 Basics of ISO 27000-Family . . . . .	3
2.2 Alternative and Regional ISMS Standards . . . . .	4
2.3 Requirements for an ISO-Compliant ISMS . . . . .	4
<b>3 Implementation Context</b>	<b>7</b>
3.1 Relevance of Certification as a Competitive Advantage for SMEs . . . .	7
3.2 Description of the Companies and their Structure in the Specific Consulting Branch . . . . .	9
3.3 Requirements and Challenges in ISMS Implementation for the Companies in Scope . . . . .	10
<b>4 Proposed Solution</b>	<b>11</b>
4.1 Development of a Process Model . . . . .	11
4.1.1 Plan . . . . .	11
4.1.2 Do . . . . .	15
4.1.3 Check . . . . .	20
4.1.4 Act . . . . .	21
4.2 Reference Implementation of the ISMS in the Company Context . . . .	22
4.2.1 Git Approach . . . . .	22
4.2.2 GitLab Approach . . . . .	23
4.2.3 Interoperability: Technologies . . . . .	24
4.2.4 Transparency and Ease-of-Use . . . . .	24
<b>5 Implementation and System Operation</b>	<b>26</b>
5.1 ISMS Documentation in Practice . . . . .	26
5.1.1 Structure and Mapping Strategy . . . . .	26
5.1.2 Policy Consolidation and Public-Facing Structure . . . . .	27
5.2 Living Processes via GitLab . . . . .	29



5.2.1	GitLab Issue System . . . . .	29
5.2.2	Tagging and Filtering System . . . . .	31
5.2.3	Board-Based Organization . . . . .	33
5.2.4	Issue Templates . . . . .	34
5.2.5	Real-World Examples . . . . .	35
5.3	Integration of Tooling and Workflow . . . . .	36
5.3.1	Workflow Integration . . . . .	36
5.3.2	Seamless Fit into Daily Operations . . . . .	36
5.3.3	Tool Adoption Across User Types . . . . .	37
5.4	Internal and External Audit Execution . . . . .	37
5.4.1	Internal Audit Process . . . . .	37
5.4.2	Handling of Non-Conformities and Recommendations . . . . .	38
5.4.3	External Audit Process (Certification Audit) . . . . .	38
5.4.4	Management Review . . . . .	38
5.4.5	Post-Audit and Review Integration . . . . .	39
<b>6</b>	<b>Lessons Learned, Audit Insights and Transferable</b>	
	<b>Recommendations</b>	<b>40</b>
6.1	General Feedback on the Use of Git . . . . .	40
6.2	Applicability of the Process Model . . . . .	41
6.3	Feasibility of the Reference Implementation . . . . .	41
6.3.1	Documentation and Policy Consolidation . . . . .	41
6.3.2	Access Control and Separation of Sensitive Areas . . . . .	41
6.3.3	Recurring Tasks and Process Maintenance . . . . .	42
6.4	Audit Insights . . . . .	42
6.4.1	Internal Audit . . . . .	42
6.4.2	External Certification Audit . . . . .	42
6.5	Transferable Recommendations for Similar SMEs . . . . .	43
<b>7</b>	<b>Conclusion</b>	<b>45</b>
<b>8</b>	<b>Appendix</b>	<b>47</b>
8.1	Examples from Issue Templates . . . . .	47
8.1.1	Risk Assessment Template . . . . .	47
8.1.2	Risk Treatment Template . . . . .	50
8.1.3	General Measure Template . . . . .	51
8.2	Examples from Implementation . . . . .	52
8.2.1	Risk Assessment . . . . .	52
8.2.2	Audit Finding . . . . .	53
8.2.3	Improvement Suggestion . . . . .	54

8.2.4 Topic-Specific Issues . . . . .	55
8.3 Acknowledgment of Company Support . . . . .	56
<b>Abbreviations</b>	<b>57</b>
<b>Bibliography</b>	<b>58</b>
<b>List of Figures</b>	<b>60</b>

# 1 Introduction

ISO/IEC 27001:2022 is an internationally recognized standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It specifies requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). The “:2022” suffix identifies the edition year of the standard and reflects the set of requirements and controls defined in that revision. Certification to this standard demonstrates an organization’s commitment to protecting the confidentiality, integrity, and availability of information assets through a structured, continuously improving ISMS.

## 1.1 Problem Statement and Objectives

ISMSs are essential for achieving compliance with ISO/IEC 27001:2022, particularly in the context of Small and Medium-sized Enterprises (SMEs) [1]. However, SMEs operating in IT security consulting often face significant challenges when implementing an ISMS effectively. These challenges are typically caused by limited resources, the lack of dedicated compliance teams, and the complexity of the standard’s requirements.

This thesis proposes a framework and reference implementation for an ISMS based on Git and GitLab. Compared to traditional ISMS tools (e.g., document-based systems, Excel tracking, or enterprise compliance suites), Git and GitLab offer several advantages for SMEs: they are open source, widely known in technical teams, and support version control, collaboration, and traceability out of the box. The decision is influenced by the technical culture of the company, the desire for full transparency, and the need to minimize tool overhead. A detailed rationale and alternative considerations are discussed in Section 4 (see page 11).

The goal is to deliver a practical, scalable solution tailored for SMEs that fully aligns with ISO/IEC 27001:2022 requirements while remaining maintainable in day-to-day operations.

## 1.2 Structure and Methodology

The thesis follows a structured approach to accompany, analyze, and document the implementation of an ISMS in a real-world SME context. It applies a methodology focused on designing and evaluating reference implementations of processes and artifacts to address practical challenges in a rigorous and transferable way, following principles of Design Science Research (DSR) [2].

In this context, the Git-based ISMS serves as the artifact: a lightweight, modular, and auditable system designed for SMEs. The thesis documents the decision-making steps involved in the system's development, evaluates its effectiveness, and explores its broader applicability.

The structure of the thesis is as follows:

- **Section 1** (current chapter) introduces the problem statement, the objectives of the thesis, and the applied structure and methodology.
- **Section 2** introduces the theoretical foundations, including the ISO/IEC 27000 series and core ISMS requirements.
- **Section 3** presents the organizational and operational context of the SME in scope and identifies relevant implementation challenges.
- **Section 4** outlines the proposed solution, including the process model and reference implementation.
- **Section 5** describes the implementation and system operation, focusing on real-world integration and tooling.
- **Section 6** summarizes lessons learned, audit insights, and transferable recommendations for similar organizations.
- **Section 7** highlights the key findings, confirms feasibility, and evaluates the transferability of the approach for technically capable SMEs.

## 2 Theoretical Foundations: ISO/IEC 27000:2022 and ISMS

Information security management relies on established frameworks and standards to provide consistency, assurance, and guidance across organizations of all sizes. This chapter introduces the theoretical foundations relevant to the development of an ISMS for SMEs, with particular emphasis on the ISO/IEC 27000 series and related standards that form the core basis for certification and compliance.

### 2.1 Basics of ISO 27000-Family

The ISO/IEC 27000 series defines internationally recognized standards for establishing, implementing, and continually improving an ISMS. At its core is ISO/IEC 27001:2022, which specifies the formal requirements for a certifiable ISMS [3]. It outlines the management system framework and mandates the implementation of appropriate information security controls through a structured, risk-based process.

Several supporting standards complement the core specification. ISO/IEC 27002:2022 provides detailed guidance on the selection and implementation of information security controls [4]. ISO/IEC 27003:2017 describes best practices for planning and implementing an ISMS [5]. ISO/IEC 27005:2018 focuses specifically on the risk management processes necessary for effective information security [6]. Additionally, ISO/IEC 27701:2019 extends the ISMS framework to address privacy information management [7].

For SMEs, it is important to note that certification is based solely on compliance with ISO/IEC 27001. Although supporting standards offer valuable guidance to facilitate effective implementation and organizational maturity, only the fulfillment of ISO/IEC 27001—including its management system requirements and the Statement of Applicability—is formally assessed during the certification process [1].

In practice, naming conventions such as *DIN ISO/IEC* or *ISO/IEC EN* reflect the adoption of international standards at national or European level. For the purposes of this thesis, the unified abbreviation “ISO/IEC” will be used consistently.

## 2.2 Alternative and Regional ISMS Standards

ISO/IEC 27001 serves as the global benchmark for ISMS certification. Nonetheless, other frameworks and standards are commonly encountered—especially by SMEs seeking simplified entry points, phased adoption, or regionally aligned solutions.

- **ISO 9001** focuses on quality management and is frequently implemented alongside ISO/IEC 27001 to demonstrate process reliability and continuous improvement in organizations [8].
- **BSI IT-Grundschutz** is a German ISMS framework designed for flexibility and practical use in public institutions and SMEs. It features a modular structure with predefined building blocks (*Bausteine*) and measures (*Maßnahmen*) [9]; [10]; [11]. Its “standard security level” approach facilitates implementation but may be too generic for specialized IT security consulting companies.
- **VdS 10000** provides a pragmatic cybersecurity standard tailored for SMEs. It focuses on a reduced control set and prescriptive implementation support, serving as an accessible alternative or preparatory step for ISO/IEC 27001.
- **ISIS12** (Information Security in Twelve Steps) offers a structured and manageable entry-level ISMS model, particularly suited for municipalities or small organizations. Its phased approach promotes adoption over time and may serve as a stepping stone to full ISO compliance.

These alternatives offer value in specific scenarios or regulatory environments but are not interchangeable with ISO/IEC 27001 in terms of international certification and acceptance. They may complement or precede ISO adoption, but do not replace the formal scope of ISO/IEC 27001 [1].

## 2.3 Requirements for an ISO-Compliant ISMS

ISO/IEC 27001:2022 defines a structured set of requirements for establishing, operating, and continually improving a certifiable ISMS [3]. These requirements are designed to be applicable to organizations of all sizes, but present specific challenges and opportunities for SMEs [1].

The clause structure of the standard forms the normative basis for ISMS certification and is consistently referenced in this thesis using official clause numbers and designations. The following figure summarizes these main clauses to provide an overview for orientation.

Clause 4 – Context of the Organization
Clause 5 – Leadership
Clause 6 – Planning
Clause 7 – Support
Clause 8 – Operation
Clause 9 – Performance Evaluation
Clause 10 – Improvement
Annex A – Information Security Controls Reference

Figure 1: Clause Structure of ISO/IEC 27001:2022

The following subsections highlight core components of these clauses:

- **Context Analysis**

Organizations must define the scope of the ISMS and analyze internal and external issues (Clause 4.1), including legal, regulatory, and contractual obligations, as well as the expectations of relevant stakeholders (Clause 4.2). Furthermore, top management must demonstrate leadership and commitment to information security (Clause 5.1) and define roles, responsibilities, and authorities (Clause 5.3).

- **Risk Management**

A central element of ISO/IEC 27001 is the identification, evaluation, and treatment of information security risks (Clauses 6.1.2 and 6.1.3). This process guides the selection of controls and must be repeatable, consistent, and aligned with the organization's risk appetite [6].

- **Security Objectives and Controls**

Organizations must define measurable security objectives (Clause 6.2) and establish appropriate Key Performance Indicators (KPIs). Based on risk assessments and requirements management, applicable controls are selected from *Annex A* of the standard and documented in the Statement of Applicability (SoA) (Clauses 6.1.3 d and 8.1).

- **Continuous Improvement and Performance Evaluation**

The ISMS must operate under a continuous cycle of evaluation and improvement (Clauses 9 and 10). This includes regular internal audits, management reviews, and corrective actions to ensure adaptability and long-term sustainability.

- **Documentation and Evidence**

Certification requires structured documentation—such as policies, procedures, audit records, and risk logs—that demonstrate intent and implementation (Clauses 7.5 and 9.2). These records ensure traceability, accountability, and transparency throughout the ISMS lifecycle.

For SMEs, these requirements must be balanced with limited resources and operational constraints. A lean, technology-supported approach—such as version-controlled documentation and integrated task-tracking—can help meet compliance goals without introducing unnecessary overhead [1], [12].



## 3 Implementation Context

This chapter describes the organizational and operational environment in which the ISMS implementation took place. It highlights the relevance of ISO/IEC 27001 certification as a competitive factor for SMEs in IT security consulting, explains the typical company structure in this sector, and outlines specific challenges faced during ISMS setup.

Understanding this context is essential for evaluating the feasibility and design decisions of the proposed solution. These considerations directly inform the implementation approach developed in Section 4.

### 3.1 Relevance of Certification as a Competitive Advantage for SMEs

SMEs, as defined by the European Commission, are organizations with fewer than 250 employees and either an annual turnover of up to €50 million or a balance sheet total of up to €43 million [13]. Within this category, small enterprises are defined as having fewer than 50 employees and a turnover or balance sheet total of no more than €10 million. This classification is widely used for determining eligibility for support programs and regulatory expectations and serves as a standard reference for economic analysis in the European context.

The IT security consulting sector emerged in the late 1980s and early 1990s, as organizations began to recognize the need for specialized expertise to secure increasingly complex and interconnected IT environments. Initially, technical knowledge and niche skills were often sufficient to establish market presence, with consulting engagements focused primarily on infrastructure hardening and network security. Over time, the landscape evolved—driven by the rise of the internet, digital business models, cloud infrastructure, and a growing dependence on information systems. As a result, regulatory expectations and client demands increased, and formal standards like ISO/IEC 27001 have become important signals of operational maturity, trustworthiness, and strategic competence.

Today, the global cybersecurity services market—including consulting, penetration testing, risk assessment, and compliance support—continues to grow significantly. The cybersecurity consulting segment is widely regarded as a growing market, driven by rising regulatory expectations, client assurance demands, and the increasing strategic relevance of cybersecurity. While concrete market size estimates vary depending on the scope and segmentation of services included<sup>1</sup>, the overall trend indicates a sustained expansion of the sector.

This development spans thousands of providers worldwide—from boutique consultancies to multinational firms—and reflects a broader shift from purely technical engagements toward integrated, risk-based approaches that embed security into organizational strategy and governance.

For SMEs in this sector, certification represents more than just compliance—it is rapidly becoming a baseline expectation for market participation. While large consulting firms benefit from brand recognition and economies of scale, SMEs must demonstrate professionalism and adherence to internationally recognized standards. Certification not only strengthens credibility and transparency but increasingly determines eligibility for contracts and long-term client relationships.

In the specific case of the company examined in this thesis, demand for ISO/IEC 27001 certification arose directly from client expectations, as reported internally by the Chief Executive Officer (CEO). While existing client relationships had tolerated informal assurance mechanisms, both renewals and new engagements increasingly required formal evidence of ISMS compliance. In particular, procurement procedures in larger client organizations often mandated ISO certification as a prerequisite for vendor selection or continued cooperation.

Although the lack of certification had not affected day-to-day operations prior to 2025, the risk of losing key clients during contract renewal was deemed too high. Postponing certification until it was formally demanded posed an additional risk, due to the lead time required for planning, implementation, and audit preparation. A delayed response could jeopardize business continuity and lead to competitive disadvantage.

Pursuing ISO/IEC 27001 certification is therefore not merely a compliance initiative but a proactive response to shifting market requirements—and a strategic investment in long-term viability within the IT security consulting domain.

---

<sup>1</sup>Exact figures differ by source and methodology; however, all major market analyses agree on substantial year-over-year growth, especially in the cybersecurity consulting segment.

## 3.2 Description of the Companies and their Structure in the Specific Consulting Branch

The IT security consulting sector includes a diverse range of organizations. A notable portion consists of SMEs that specialize in the provisioning of technical services, such as penetration testing, vulnerability assessments, and security architecture consulting. These companies tend to be stable but not fast-growing, maintaining a consistent client base over extended periods.

Organizationally, such SMEs often operate with small teams—sometimes fewer than 15 employees—occasionally supported by external contractors or freelancers. They feature a flat hierarchy, with no dedicated departments. Core business and administrative responsibilities are usually concentrated in the hands of the CEO or a few key individuals, which complicates resource planning and the formalization of structured processes.

The operational focus lies strongly on technical service delivery, while support processes—such as Human Resources (HR), quality management, or formal documentation—are kept to a practical minimum, while guaranteeing legal compliance. Employees typically possess strong technical expertise, including familiarity with industry standards such as Request for Comments (RFCs) and ISO/IEC norms relevant to information security.

A common characteristic among companies in this sector is the need for technological autonomy. Consultants often manage their own systems or tool sets. Traditional, centralized enterprise ISMS platforms may therefore be seen as too rigid, introducing overhead that conflicts with agile and technically autonomous work environments.

An effective ISMS in this context must balance structure and compliance with flexibility and minimal management effort—without compromising security requirements. The *ISO/IEC 27001:2022 ISMS Practical Guide for SMEs* emphasizes that ISO/IEC 27001 is a flexible and scalable standard and that ISMS implementation should not result in excessive rules, bureaucracy, or financial burden [1]. Instead, it should be regarded as an investment that strengthens information security and improves business resilience.

This perspective supports the development of lightweight, adaptable ISMS implementations tailored to SME-specific needs, as exemplified by the Git-based approach described in this thesis.

### 3.3 Requirements and Challenges in ISMS Implementation for the Companies in Scope

Implementing an ISMS in small, technically skilled consulting companies presents a distinct set of requirements and challenges. While the initial investment in time and resources is typically manageable, long-term success depends on designing a system that is sustainable and efficient with minimal overhead.

In the company examined in this thesis, the ISMS team was intentionally kept lean, consisting of:

- a **Chief Information Security Officer (CISO)** (also handling other technical roles), who maintained and developed the ISMS part-time,
- the **CEO**, involved due to their direct oversight of most operational processes,
- and a **technical administrator** (“Admin”), responsible for the practical implementation of controls at system level.

This structure reflects the constraints and pragmatism typical of SMEs in this sector and informs the implementation approach described in the following chapters.

The ISMS is intended to fulfill not only certification requirements but also serve as a tool for internal process improvement. One of its immediate benefits lies in documenting and formalizing practices that already exist informally. This enables a gap analysis, identifying where additional processes, responsibilities, or controls are required to meet ISO/IEC 27001 standards.

In some cases, SMEs may benefit from engaging external consultants to support ISMS setup—particularly when in-house capacity or compliance experience is limited. However, this depends on budget, available time, and organizational culture.

Change management, however, poses a notable challenge. Teams accustomed to informal or autonomous workflows may resist process formalization. Transitioning from operational freedom to documented, repeatable procedures can be perceived as bureaucratic overhead. Additionally, differences in security expectations—between staff aiming for best practices and those focused on minimum compliance—can create friction.

A successful ISMS in this environment must therefore strike a balance between compliance needs and cultural fit, minimizing disruption while enabling long-term process maturity.

The following chapter presents a tailored ISMS solution, designed with these constraints and requirements in mind.

## 4 Proposed Solution

The following chapter presents a tailored ISMS framework, designed to address the specific challenges identified in the preceding implementation context. Building on ISO/IEC 27001:2022 requirements, the approach is structured around the Plan-Do-Check-Act (PDCA) cycle, and leverages Git- and GitLab-based tooling for transparent, scalable implementation. The process model and reference implementation are explained in detail across the subsequent sections.

### 4.1 Development of a Process Model

The proposed ISMS framework follows the PDCA cycle, a widely recognized management model for systematic process control and continuous improvement. While ISO/IEC 27001:2022 does not mandate PDCA specifically, it implicitly expects organizations to operate their ISMS in a repeatable, evaluable, and adaptive manner [3]. PDCA fulfills these expectations by emphasizing structured planning, implementation, performance monitoring, and iterative refinement.

Alternative models exist and are conceptually similar, each promoting closed feedback processes. However, PDCA was selected here for its international recognition, its clear mapping to ISO clauses (e.g., Clause 10: Improvement [3]), and its widespread use in quality and security management systems.

Additionally, the PDCA structure lends itself well to modeling real-world ISMS activities in small consulting firms. It supports a balance between formal compliance and operational pragmatism, helping ensure that security measures evolve with business needs in an iterative manner.

The following subsections illustrate how each phase of the PDCA cycle maps to the concrete implementation context of the ISMS under study.

#### 4.1.1 Plan

The planning phase designs and establishes the foundational structure of the ISMS. For the company in scope, this began with a clear and practical definition of the ISMS scope and the security objectives.

### 4.1.1.1 Scope Definition

In accordance with Clause 4.3 of ISO/IEC 27001:2022 [3], the ISMS scope was defined in collaboration with the CEO and supported by external consultants. The decision to cover the entire organization was based on the compact and focused nature of the SME, where all operational activities revolve around a single core process, formally defined as:

IT security audits, workshops, and architecture reviews related to software and hardware consulting

#### Excerpt 1: ISMS Scope

Unlike larger organizations with multiple departments and support functions, the company operates without substantial support structures. This made a holistic scope both practical and advantageous for certification, as it ensures that all relevant processes and assets are included from the outset.

The agreed-upon scope is also reflected in the formal certification document, which clearly designates the component for which compliance is being demonstrated. By covering the full organization, the ISMS ensures broad and transparent protection of all relevant client and operational information.

### 4.1.1.2 Objective Definition

In line with ISO/IEC 27001:2022 Clause 6.2, measurable information security objectives were defined during the planning phase. These were developed collaboratively by the internal ISMS team—consisting of the CEO, part-time CISO, and system administrator—with support from external consultants. The selected objectives reflected both organizational priorities and the standard’s requirements to manage risks, meet stakeholder needs, and continually improve the security posture [3].

The objectives were directly derived from the company’s core business activities and were designed to strengthen and secure its central consulting process. Each objective is supported by one or more KPIs, which are used to track and evaluate effectiveness over time—primarily through risk treatment status, audit feedback, and recurring reviews.

Four key objectives were defined:

**Objective 1: Protection of Customer Data**

Ensure the Confidentiality, Integrity, and Availability (CIA) of customer data to protect it from unauthorized access, disclosure, and modification.

**Objective 2: Business Continuity**

Maintain business continuity through effective risk management and minimizing business disruptions. This includes measurable aspects within the risk management process.

**Objective 3: Internal Operational Security**

Ensure that internal processes are carried out in a secure and reliable manner to protect against operational risks and maintain the integrity of business operations.

**Objective 4: Compliance and Transparency**

Comply with applicable standards, regulations, and contractual obligations, and provide transparency towards customers with regard to information security practices.

**Excerpt 2: ISMS Objectives of the Reference Implementation**

These objectives are subject to periodic assessment during the management review process (Clause 9.3) and may be adjusted based on audit results, changes to business strategy, or evolving risk exposure [3].

### 4.1.1.3 Initial Risk Assessment

A two-layered risk assessment approach was adopted to ensure both baseline coverage and asset-specific focus. This strategy was chosen to balance thoroughness with maintainability, which is particularly relevant in a small consulting environment.

First, a general baseline was established using **G0-threats**—also known as **elementary threats** (*Elementare Gefährdungen*) from the BSI IT-Grundschutz framework [11]. These represent a standardized set of foundational threat types, e.g., fire, data loss, power failure, and provide broad coverage across general operational risks.

Second, targeted risk assessments are performed for specific core assets critical to business operations—such as customer data repositories, administrative tools, and internal communication systems. These assessments include threat identification,

risk estimation, and treatment planning as required by ISO/IEC 27001 Clauses 6.1.2 and 6.1.3 [3].

This dual-layer approach ensures that both generic and context-specific risks are captured without overburdening the ISMS team with overly complex modeling requirements.

### 4.1.1.4 Selection of Controls

In the early implementation phase, all controls from *Annex A* were initially marked as applicable. This decision was based on the assumption that—in a small, technically specialized consulting company with high exposure to client data and systems—most controls would be either directly relevant or easily adaptable.

This “include-all-then-reduce” approach simplified the initial gap analysis by reducing the risk of overlooking essential controls. It also supported awareness-building, as the ISMS team explicitly reviewed and assessed each control’s applicability.

In later stages, certain controls could be excluded or marked as not applicable, with documented justification (e.g., physical site protection for unused locations).

This approach ultimately helps to streamline the SoA process while ensuring completeness and defensibility during internal and external audits.

### 4.1.1.5 Design Decisions

Two foundational design choices shape the structure and usability of the ISMS:

- The use of a Git-based documentation model. Git is a distributed Version Control System (VCS) designed to track changes in files, support collaboration across teams, and ensure traceability over time. Its lightweight yet powerful architecture enables parallel workflows, precise versioning, and detailed change histories, making it ideal for environments where technical teams require flexibility without the burden of traditional document management systems. At the SME at hand, Git already is a familiar and widely adopted technology. Employing it into the realization of the ISMS further helps minimizing additional operating and maintenance costs while supporting efficient, transparent collaboration.
- A structured mapping strategy is implemented, where each ISO clause and control is assigned its own dedicated Markdown file. This modular architecture improves transparency, simplifies internal audits, and enables easy cross-referencing and maintenance. It also supports automated change tracking and file-based SoA mapping.



These design decisions were evaluated in cooperation with the CEO and external consultants. Simpler options—such as flat Word/Excel documents or shared drives—were considered but rejected due to limitations in traceability, versioning, and integration with Issue-based process tracking.

Furthermore, the company already maintained procedural and security-related documentation in a centralized location commonly referred to as the “Handbook.” To avoid fragmentation and build on existing structures, it was decided to integrate the ISMS directly into this handbook. This decision allowed for a unified documentation approach, minimizing redundancy and improving accessibility for all team members.

It also creates an opportunity to embed ISMS-relevant regulations, guidelines, and informative content seamlessly into existing handbook sections. For example, general company procedures can now include embedded security requirements or link directly to corresponding controls—fostering both usability and awareness.

The “Plan” phase thus established a lean yet comprehensive ISMS structure tailored to the needs and resources of a highly specialized SME environment.

### 4.1.2 Do

In the “Do” phase, the planned structure and design of the ISMS are operationalized. This includes the implementation of ISO/IEC 27001 clauses, the adoption of *Annex A* controls, the preparation of supporting documentation, and the formalization of the design decisions made in the planning phase.

#### 4.1.2.1 Implementation of Chapters and Controls

Each relevant clause of ISO/IEC 27001:2022 and the corresponding ISO/IEC 27002 control groups are implemented through dedicated Markdown files, a lightweight markup format that enables easy, readable documentation. These documents define the necessary policies, procedures, and practices in a modular and maintainable format.

The file structure is deliberately designed to be granular, improving traceability, facilitating audits, and simplifying long-term maintenance. Each ISO/IEC 27001 clause and its associated controls are directly mapped to specific Markdown files, resulting in the following directory layout within the Git-based ISMS repository:

ISO Chapter 4 - Context of the Organization in directory tree:  
    /ISMS/4. Context of the Organization

ISO Chapter 5 - Leadership in directory tree:  
    /ISMS/5. Leadership

ISO Chapter 6 - Planning in directory tree:  
    /ISMS/6. Planning

ISO Chapter 7 - Support in directory tree:  
    /ISMS/7. Support

ISO Chapter 8 - Operation in directory tree:  
    /ISMS/8. Operation

ISO Chapter 9 - Performance Evaluation in directory tree:  
    /ISMS/9. Performance Evaluation

ISO Chapter 10 - Improvement in directory tree:  
    /ISMS/10. Improvement

ISO 27001 Annex A (ISO 27002 recommendations) in directory tree:  
    /ISMS/A5 Organizational Controls  
    /ISMS/A6 People Controls  
    /ISMS/A7 Physical Controls  
    /ISMS/A8 Technological Controls

Condensed policy and reusable content structure:  
    /ISMS/Policies  
    /ISMS/AX Policy Includes

#### Excerpt 3: Clause Mapping

As illustrated above, this modular layout closely mirrors the structure of ISO/IEC 27001. It ensures that documentation remains intuitive, auditable, and scalable over time. It allows auditors and internal stakeholders to directly trace the implementation of each clause and control, while facilitating cross-linking of guidance, roles, and responsibilities.

#### 4.1.2.2 Policy Development

Policies are derived directly from the requirements defined in the ISO/IEC 27001 clauses and the applicable *Annex A* controls. Depending on complexity and relevance, policies are either embedded within the relevant Markdown files or referenced as standalone documents. This modular design supports clarity, simplifies auditing, and allows individual components to be updated independently.

ISO/IEC 27002:2022 introduces the concept of 14 *topic-specific policies* to group and formalize related control areas (e.g., *Acceptable Use of Information*, *Access Control*, *Data Retention*) [4]. In practice, implementing a strict one-to-one mapping of policies to all 14 topics would introduce unnecessary overhead in a SME context.

Therefore, controls are reviewed and clustered into a leaner, more maintainable structure.

As a result, six major policies are defined. These cover all essential information security aspects while remaining maintainable within the company's resource and organizational constraints. The following list reflects actual filenames and titles from the Git-based ISMS repository, formatted for internal consistency and audit traceability:

### Top Level Policies

- [Information Security Policy] (Clause 5.2)

### Topic-specific Policies

- [Policy - Core Process IT Security Consulting]
- [Policy - External Contractors]
- [Policy - Internal Software Development]
- [Policy - Working with Hardware and Software for Consulting Tasks]
- [Policy - Working with Hardware and Software for General Operation ("Infrastructure")]

Excerpt 4: ISMS Policies

Each policy addresses a specific operational or strategic aspect:

- **Information Security Policy:** Defines the overall information security objectives, the purpose of the ISMS, and the commitment of top management (Clause 5.2 [3]).
- **Core Process IT Security Consulting:** Describes the secure handling of client projects, including project scoping, communication, documentation, and delivery.
- **External Contractors:** Specifies requirements for external suppliers and freelancers, enabling effective supplier contract and relationship management, facilitating secure collaboration.
- **Internal Software Development:** Outlines baseline controls and secure development practices for internal tooling. Although the company does not develop commercial software, internally developed tools (e.g., scripts, dashboards) are covered by the ISMS.
- **Hardware and Software for Consulting Tasks:** Establishes rules for equipment directly assigned to employees (e.g., laptops, consulting toolkits) used in customer-facing work.

- **Hardware and Software for General Operation (“Infrastructure”):**  
Covers infrastructure components not directly used in consulting projects, such as office systems, admin devices, and backend services.

This policy set provides structured, auditable coverage of all relevant areas, while remaining manageable within the operational context of a small, highly specialized consulting firm.

### 4.1.2.3 Assignment of Responsibilities

In accordance with ISO/IEC 27001:2022, Clause 5.3, roles and responsibilities within the ISMS are clearly defined and assigned [3]. The aim is to ensure that all relevant security-related processes have a respective owner assigned, while aligning with the company’s flat hierarchy and limited personnel.

The ISMS role model includes:

- The **CISO** (part-time), responsible for coordinating ISMS development and maintenance, facilitating audits, and managing internal reviews.
- The **CEO**, accountable for overarching ISMS governance, strategic direction, and approval of major policy and risk decisions.
- The **Admin** (technical staff), with clearly delegated responsibilities for specific controls, such as backups, system hardening, access reviews, and incident response.

To support differentiated access control and process transparency, several additional functional roles are defined, including:

- **DPO** (Data Protection Officer),
- **OPS** (Project Management Team),
- **SwDev** (Internal Tooling Development Team),
- **Trainer** (Technical Workshop Instructors).

These roles reflect functional distinctions within the small team and prepare for differentiated access controls. For instance, **SwDev** roles are granted write access to internal code repositories, **OPS**—by default—can access all client-related projects, and **Trainers** may request access to specific project repositories to retrieve materials for workshops.

All roles and their responsibilities are documented directly within the mapping file associated with Clause 5.3, ensuring tight integration between process documentation, ownership, and technical access control. This alignment between documentation and technical enforcement further enhances audit readiness and compliance transparency.

### 4.1.2.4 Implementation and Design of Processes

The implementation of ISMS processes follows a hybrid approach: static documentation ensures transparency and completeness, while dynamic task tracking enables execution and accountability.

All core ISMS processes are documented in a central mapping file located at:

`/ISMS/8. Operation/8.1 Operational Planning and Control.md`

This file defines the structure and responsibilities for key ISMS operational activities, including:

- ISMS Governance and Strategic Planning
- Asset Management
- Risk & Opportunity Identification & Treatment
- Controls and Document Management
- Training and Awareness
- Internal Audits and Security Performance Monitoring
- Management Reporting and Review
- Tracking, Correction, and Continuous Improvement
- Security Incident Management & Emergency Preparedness

Each process entry outlines its purpose, inputs and outputs, responsible and accountable roles, and any associated sub-tasks or dependencies. This centralized structure ensures that all major activities are transparently defined and auditable in a single location, aligned with ISO/IEC 27001 Clause 8.1 [3].

However, static documentation alone does neither enable real-time planning nor execution. To operationalize the processes, GitLab Issues are used—serving as structured, actionable tasks with assigned responsibilities and defined timelines (e.g., due dates, reminders). Depending on the nature of the task, Issues may represent individual process steps or consolidate related activities into collective “planning Issues”. For details on the Issue system and templates, see Section 5.2 (page 29).

This combination allows for both structural clarity and operational flexibility:

- The **static mapping file** serves as the definitive reference for defined processes.
- The **GitLab Issue system** enables real-time planning, delegation, and progress tracking.

Together, these components ensure compliance while maintaining practical feasibility within the constraints of a small consulting organization.

### 4.1.3 Check

The “Check” phase focuses on evaluating the performance and effectiveness of the ISMS. This is achieved through ongoing monitoring, structured internal audits, regular management reviews, and formal assessments of implemented controls, in line with ISO/IEC 27001:2022 Clauses 9.1 and 9.3 [3].

- **Monitoring and Auditing:**

Continuous monitoring of ISMS-related processes is supported through GitLab Issue tracking and labeling, providing transparency into open risks, recurring tasks, and control implementations.

Formal assessments are conducted through:

- Internal audits (at least annually),
- Management reviews (at least annually),
- Surveillance or certification audits (by accredited external bodies).

These activities ensure that each ISMS clause, control, policy, and identified risk is reviewed regularly. The audit scope typically includes the full cycle of Information Security Risk Management (ISRM), evaluation of all documentation, and performance tracking against defined objectives and KPIs. Audit findings are categorized into major/minor non-conformities and Opportunity for Improvements (OFIs), all of which are fed into the backlog tracked via GitLab Issues.

- **Management Reviews:**

Management reviews are conducted periodically—at minimum once per year—and are led by the CEO and the CISO. The reviews evaluate the ISMS’ performance using KPIs, objective fulfillment, audit results, and changes in business or threat context. Corrective actions and improvement recommendations are derived from these review sessions and are documented accordingly.

- **Effectiveness of Measures:**

All implemented controls and risk treatments are regularly assessed for effectiveness, including reviewing whether identified risks were sufficiently mitigated and if new risks have emerged. Where required, corrective actions are initiated and tracked as GitLab Issues.

- **Evidence Tracking:**

All reviews, audit findings, evaluation results or any other outcome worth documenting is recorded in version-controlled Markdown reports or logged as Issues in GitLab, ensuring traceability and follow-up across all review phases.

While internal audits are process- and documentation-focused, external audits additionally validate certification readiness and conformity with third-party expectations.

This structured review process ensures that the ISMS remains aligned with both compliance requirements and business objectives, while forming a feedback loop that directly informs improvements in the “Act” phase.

### 4.1.4 Act

The “Act” phase closes the PDCA cycle by initiating improvements based on evaluations and feedback from the “Check” phase. This aligns with ISO/IEC 27001:2022 Clause 10, which mandates actions to address non-conformities and drive continual improvement [3].

- **Addressing Improvements:**

Internally identified issues—such as process deviations, inefficiencies, outdated documentation, or low control effectiveness—are addressed through structured improvement tasks. These tasks are managed as GitLab Issues with assigned responsibilities and due dates, ensuring traceability and accountability across the ISMS lifecycle.

- **Refining Based on Feedback:**

Insights from internal audits, management reviews, or recurring issues discovered through ongoing monitoring are reviewed, discussed, and translated into updates to ISMS documentation, controls, and processes as needed.

- **Responding to Change:**

Changes in the organizational context (e.g., new services, personnel or supplier changes, or regulatory shifts) and developments in the external threat landscape are integrated by updating the risk register, reassessing relevant controls, and modifying affected procedures or policies.

All improvement actions are documented either directly in the Git-based ISMS or tracked as Issues in GitLab. This ensures transparent linkage between findings and follow-up actions, supporting continuous development and audit readiness.

The outcomes from this phase are fed directly into the next planning cycle, ensuring the ISMS continually evolves and remains aligned with organizational needs and external requirements.

## 4.2 Reference Implementation of the ISMS in the Company Context

This section presents the practical realization of the proposed ISMS framework within the operational environment of the company. Building on the principles and design decisions outlined previously, the implementation leverages existing technical capabilities—particularly Git and GitLab—to create a lightweight, maintainable, and audit-ready ISMS.

The subsections describe the technological foundations, interoperability considerations, and usability strategies that shaped the system’s final design.

### 4.2.1 Git Approach

At the core of the reference implementation is a Git-based documentation model. This approach leverages **Git as a version control system** to manage all ISMS artifacts, including policies, risk assessments, and procedures.

Git was selected due to its widespread use within the company, its technical robustness, and its support for distributed collaboration. The organization already relied on Git for software development and documentation management, making it a natural fit that required no new infrastructure or extensive training.

All ISMS documentation is authored in Markdown format and maintained within a Git repository. This ensures structured, consistent, and traceable information management across all documents. Git’s version history provides a complete audit trail of all changes, including authorship, timestamps, and commit messages. Where required, signed commits are used. Signed commits in Git and GitLab use cryptographic signatures (typically PGP or SSH keys) to verify the identity of the person who created a commit. This ensures the authenticity and integrity of the commit, providing assurance that it was authored by a trusted contributor and has not been tampered with, reinforcing accountability.

The ability to review incremental document changes via so-called *diffs* facilitates transparency during audits, simplifies internal reviews, and provides traceability for the evolution of risk treatments and policy updates. A *diff* displays the differences between two versions of files, highlighting added, modified, or removed content. They provide a clear view of changes made over time, helping users review updates, track revisions, and collaborate effectively on evolving information.

By building on an established, familiar toolset, the ISMS implementation avoids external dependencies, minimizes complexity, and creates a transparent, techni-



cally robust documentation environment tailored to the needs and capabilities of SMEs.

### 4.2.2 GitLab Approach

To extend the Git-based documentation model into a fully manageable ISMS environment, GitLab was integrated as the platform of choice, already in use within the company<sup>2</sup>. GitLab enhances Git repositories with collaborative features and operational tooling that support tracking, responsibility management, and structured process execution.

Several GitLab features were leveraged to operationalize the ISMS:

- **Centralized Repository for Documentation:**

The Git repository hosts all written ISMS content, including ISO clause and control mappings, policies, and documented processes. This creates a single, authoritative source of truth for the entire ISMS.

- **Living Processes via GitLab Issues:**

All dynamic or recurring ISMS activities—such as internal audits, risk reviews, corrective actions, and improvement initiatives—are managed using GitLab Issues. These are structured with labels, milestones, and Issue Boards, enabling task prioritization, responsibility assignment, and deadline tracking.

- **Seamless Integration with Consulting Workflows:**

GitLab unifies documentation and task tracking within a single platform, reducing tool fragmentation and aligning naturally with the company’s consulting-centric workflows. This integration enables transparency, consistency, and audit readiness without introducing additional overhead.

GitLab was selected based on its open-source availability (GitLab CE), native support for Git, and its prior use within the organization. This choice minimizes not only additional infrastructure or licensing-related cost, but primarily the learning curve while providing all required ISMS lifecycle management capabilities in a single environment.

The result is a practical, maintainable setup—well-suited for small teams with limited administrative capacity but strong technical foundations.

---

<sup>2</sup>While GitLab CE was used in this implementation, similar platforms such as Gitea or Forgejo—which also enhance Git with ticketing systems, project boards, and user management—could serve as alternatives depending on organizational preferences and infrastructure constraints.

### 4.2.3 Interoperability: Technologies

A key advantage of the Git-based ISMS implementation lies in its technological simplicity and broad compatibility. The system was intentionally designed to minimize infrastructure requirements, reduce operational complexity, and avoid vendor lock-in—making it particularly suitable for SMEs environments.

- **Open Licensing and Vendor Independence:**

The solution relies on **Git** (licensed under GPLv2) and **GitLab Community Edition (CE)** (licensed under the MIT License) [14], [15]. Both tools are available under permissive open-source licenses, granting full control over hosting, updates, and data ownership. This ensures that the ISMS remains cost-efficient, adaptable, and legally robust for long-term commercial use.

- **Cross-Platform Compatibility:**

Git and GitLab are platform-agnostic and accessible across all major operating systems. Most day-to-day operations—including document editing, version tracking, and Issue management—can be performed entirely through the GitLab Web interface. This approach ensures usability even for non-developers with basic technical skills, while also offering full Command Line Interface (CLI) support for advanced users.

- **Lightweight Requirements and Format Independence:**

All ISMS documentation is maintained in plain text (Markdown), with a structured mapping between ISO clauses, controls, and directory layout. This modular design guarantees long-term accessibility and interoperability, regardless of the underlying infrastructure. Even if Git or GitLab were to be replaced, the documentation would remain portable and readable, facilitating migration to other systems (e.g., SharePoint, Wiki-based platforms).

This technological foundation provides the SME with the necessary flexibility, simplicity, and sustainability—while ensuring full compliance with ISO/IEC 27001 documentation requirements.

### 4.2.4 Transparency and Ease-of-Use

A core design principle of the Git-based ISMS implementation is to ensure clarity, accessibility, and simplicity for all users—regardless of technical background or organizational role.

- **Transparent Structure:**

The ISMS is organized in a modular format, with each ISO clause and *Annex A* control mapped to a dedicated Markdown file. This structure allows stakehold-

ers to navigate intuitively, facilitates targeted document reviews, and simplifies internal and external audits.

- **User-Friendly for All Roles:**

While technical staff may prefer interacting with Git via the command line, non-technical users can contribute through the GitLab web interface. This dual-mode access lowers participation barriers and fosters shared responsibility for security documentation and processes.

- **Built-In Collaboration and Accountability:**

Git and GitLab provide full version history, diff capabilities, and approval workflows. Merge requests, comments, and linked Issues ensure that every change or decision is transparently documented, reviewable, and auditable.

- **Low Maintenance Effort:**

The use of plain text (Markdown) and standard, open-source tools eliminates reliance on proprietary software or complex infrastructure. This lightweight approach ensures that the ISMS remains sustainable over time, even with minimal administrative overhead, while keeping the content easily convertible should another solution be favored in the future.

This usability-focused design supports ISO/IEC 27001's emphasis on practical applicability and continual improvement. The result is an ISMS that is approachable, auditable, and sustainable—ideally suited to the needs of a small, specialized consulting company as introduced in Section 3.

Building on the presented framework and design choices, the next chapter details the actual implementation, operationalization, and observations gathered during the deployment of the ISMS in the company context.

## 5 Implementation and System Operation

This chapter demonstrates how the defined ISMS framework was implemented in practice within the company’s operational environment. While Section 4 outlined the conceptual design and structure of the ISMS, here, the focus shifts to real-world application, behavior, and outcomes.

Key artifacts of the implementation—such as file structures, process templates, and the integration of GitLab Issues—are presented and discussed. Screenshots and excerpts provide insight into how essential processes, such as ISRM, audit tracking, and continuous improvement, are operationalized in daily practice.

### 5.1 ISMS Documentation in Practice

The ISMS documentation is fully implemented within a Git-based repository using Markdown files. Each ISO/IEC 27001 clause and *Annex A* control is mapped to a dedicated file, enabling modular documentation, clear traceability, and streamlined auditability.

The following sections provide an overview of the documentation structure, explains the rationale behind the mapping strategy, and highlights essential aspects of documentation quality, maintenance, and usability.

#### 5.1.1 Structure and Mapping Strategy

The documentation root of the ISMS resides in the subdirectory `/isms`, which is part of the broader company handbook introduced earlier (see Section 3). This integration ensures that the ISMS is both accessible and aligned with existing internal documentation practices.

Within `/isms`, two key entry points provide orientation and navigation:

- `/isms/README.md`: A general introduction intended for all readers. It acts as a visible entry point into the handbook’s user interface, offering an overview of the ISMS’ purpose, its structure, access instructions etc.

- `/isms/ISMS/README.md`: The formal ISMS root document. This file serves as the structured starting point for certification-relevant content and mirrors the layout of ISO/IEC 27001. It includes:
  - 1 Scope of this Directory
  - 2 Normative References
  - 3 Terms and Definitions
  - Links to:
    - The full clause and control mapping document
    - The 5.2 Information Security Policy
    - The policy directory

The file structure visually mirrors the ISO/IEC 27001 layout, with each clause mapped to a dedicated subdirectory. This modular design simplifies navigation, supports clause-specific documentation, and streamlines internal and external audits.

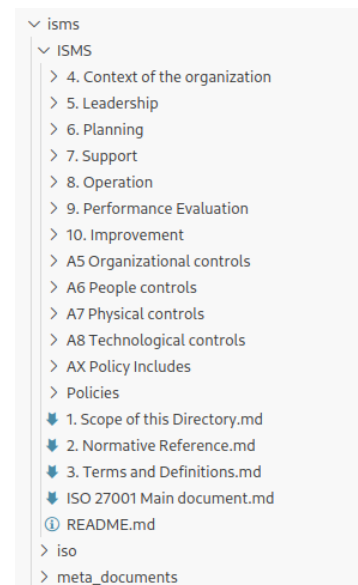


Figure 2: File Tree - `/isms`

### 5.1.2 Policy Consolidation and Public-Facing Structure

To avoid redundancy and improve maintainability, related ISO/IEC 27001 controls are often consolidated into broader, overarching policy documents. This approach presents security requirements in a more readable and actionable format.

The policies are organized into two main locations:

- `/ISMS/Policies/`: Internal policy documents. These may include references to internal control mappings or procedural documents and are primarily intended for internal use.
- `/ISMS/AX Policy Includes/`: Reusable Markdown fragments designed for inclusion in other locations (mostly in other policies, e.g., shared clauses for secure development or access control).

*Includes* refer to the ability to embed or reference the content of one file within another, allowing reusable sections (such as standard text blocks, disclaimers, or policies) to be maintained centrally and inserted where needed. While Markdown itself does not natively support includes, many static site generators or documentation platforms that use Markdown-flavored languages (like GitLab) extend it with include features to improve modularity, consistency, and maintainability of documentation. *Includes* are particularly beneficial as they can be reviewed and approved separately, eliminating the need for repeated review when reused elsewhere.

To support external publication, however, **Policy – External Contractors** was created as a standalone document without internal dependencies. Other policies may be modularized for external use in future iterations, if need be.



Figure 3: Structure - ISMS/Policies and ISMS/AX Policy Includes

Standalone documents are suitable for:

- Public hosting (e.g., company website)
- Sharing during client onboarding or due diligence
- Certification audits as self-contained evidence

Additional supporting directories are integrated both inside and outside the */ISMS/* tree to organize supplementary material without cluttering the main documentation structure. Examples include:

- */iso*: Documentation and references related to normative sources such as ISO/IEC 27001 and ISO/IEC 27002.

- `/meta_documents`: A collection of design decisions, implementation notes, and audit reports referenced in Issues or ISMS documents.
- `/ISMS/*/Documents`: Topic-specific attachments or supplemental material (e.g., internal notes, assessments, or questionnaires) stored alongside the corresponding ISO clauses or controls.

This structure supports transparency, modularity, and traceability while preserving clarity for both internal users and external auditors.

## 5.2 Living Processes via GitLab

To manage ongoing ISMS activities beyond static documentation, dynamic processes are executed through GitLab Issues. This approach provides traceability, accountability, and structured collaboration—fully aligned with ISO/IEC 27001’s continuous improvement and operational requirements.

### 5.2.1 GitLab Issue System

Each recurring or ad-hoc ISMS task—such as risk assessments, internal audits, improvement initiatives, or non-conformity tracking—is represented as an individual GitLab Issue. Each Issue typically includes:

- Assignment to a responsible role (e.g., CISO, Admin)
- Tagging with process-specific labels for classification and filtering
- Scheduling with due dates
- Linking to relevant documentation, controls, or audit findings
- (Optionally) creation from predefined templates in `.gitlab/Issue_templates/`

The following figure illustrates a typical audit-related Issue structure.

...

Handbook / Issues / #88

New look: On

Measure: Review Management Review for monitoring and measurement results (NCB04-2025)

Open

Issue created 2 months ago by John Robert Lißke

Key	Value
Status	Implemented. Effectiveness Review TBD
Source	Internal Audit 2025
Measure Owner	@john_robert_lisske
Effectiveness Review	TBD 08/2026

Measure Description

Audit Result

Monitoring and measurement results as well as the fulfilment of the security objectives are not currently part of the management review.

Measure

Implementation 2025-03-08

Assignee

John Robert Lißke

Labels

EffectivenessReview InternalAudit Measure NCB

Dates

Start: None  
Due: Aug 31, 2026

Milestone

None

Parent

None

Time tracking

Add an estimate or time spent.

2 Participants

Figure 4: Head of Exemplary Audit Issue

The Issue in Figure 4 is based on a template enforcing a consistent structure and providing clarity for ongoing management. Key characteristics include:

- Descriptive Title:**  
Measure: Review Management Review for monitoring and measurement results (NCB04-2025)  
Combines a clear action item with a traceable reference ID from the internal audit report.
- Metadata Table** (at the top of the Issue body):  
Includes fields such as:
  - Current Status
  - Source (e.g., Internal Audit)
  - Measure Owner
  - Effectiveness Review status
- Detailed Body Content:**  
Describes the measure and provides structured sections for:
  - Implementation notes and progress tracking
  - Audit follow-up responses



- Effectiveness reviews and outcomes
- **Meta Attributes:**
  - **Assignee:** e.g., John Robert Lißke, responsible for the next processing step.
  - **Labels:** e.g., Effectiveness Review, Internal Audit, Measure, NCB — for classification and board organization.
  - **Due Date:** e.g., Aug 31, 2026, ensuring deadlines for reviews or corrective actions are not overlooked.

### 5.2.2 Tagging and Filtering System

A custom tagging scheme enables fast filtering, navigation, and process reporting across all ISMS activities.

- **Process Tags:**
  - risk, opportunity, treatment
  - audit-internal, audit-external, improvement
- **Compliance Status Tags:**
  - NCA, NCB, RCM (OFI), Effectiveness Review
- **Contextual Tags:**
  - RiskITSecurityConsulting – Risks associated with the core process
  - Improvement, Internal Audit – used for dynamic filtering, board organization, and reporting
















Other labels  31			
<b>Chance</b>  Documentation / Handbook	Issue/Treatment that represents a chance in terms of risk management	☆	Subscribe ⋮
<b>EffectivenessReview</b>  Documentation / Handbook	Action item / measure is considered implemented and waiting for EffectivenessReview.	☆	Subscribe ⋮
<b>ExternalAudit</b>  Documentation / Handbook	Measure derived from an external audit result	☆	Subscribe ⋮
<b>Improvement</b>  Documentation / Handbook	Task derived from ISMS 10. Continual Improvement	☆	Subscribe ⋮
<b>InternalAudit</b>  Documentation / Handbook	Measure derived from an internal audit result	☆	Subscribe ⋮
<b>Measure</b>  Documentation / Handbook	Measure containing a task obtained from different sources of the ISMS (Regulations, Policies, Reviews, Audits)	☆	Subscribe ⋮
<b>NCA</b>  Documentation / Handbook	Major Non-Conformity from internal or external Audit: A deviation from at least one standard requirement, which fundamentally questions the functionality of the ISMS	☆	Subscribe ⋮
<b>NCB</b>  Documentation / Handbook	Minor Non-Conformity from internal or external Audit: A deviation from at least one standard requirement, which in its extent questions the functionality of the ISMS.	☆	Subscribe ⋮
<b>RCM</b>  Documentation / Handbook	Recommendation from internal or external Audit: The requirements of the standard are fulfilled, but individual aspects of implementation could be improved and thus contribute to improving the ISMS (potential for improvement)	☆	Subscribe ⋮
<b>RecurringMeasure</b>  Documentation / Handbook	Measures that remain usually open as they describe a repeating process	☆	Subscribe ⋮
<b>Reworked</b>  Documentation / Handbook	Marks a reworked item that requires a review.	☆	Subscribe ⋮
<b>Risk</b>  Documentation / Handbook	Identified Risk	☆	Subscribe ⋮
<b>RiskITSecurityConsulting</b>  Documentation / Handbook	Identified Risk that is directly associated with the core process of IT-Security Consulting (ISMS Scope) Includes: RLs general Infrastructure and procedures supporting the core process; Example: Risk results from internal pentests	☆	Subscribe ⋮
<b>RiskLevel0</b>  Documentation / Handbook	Identified Risk with Resulting Risk Level 0. Needs to be reviewed regularly.	☆	Subscribe ⋮

Figure 5: List of Labels for ISMS Issues

This system enables instant retrieval of targeted Issue subsets. For example, all internal audit results still requiring implementation (not yet under effectiveness review) can be located using a simple label filter—without navigating the full Issue Board.

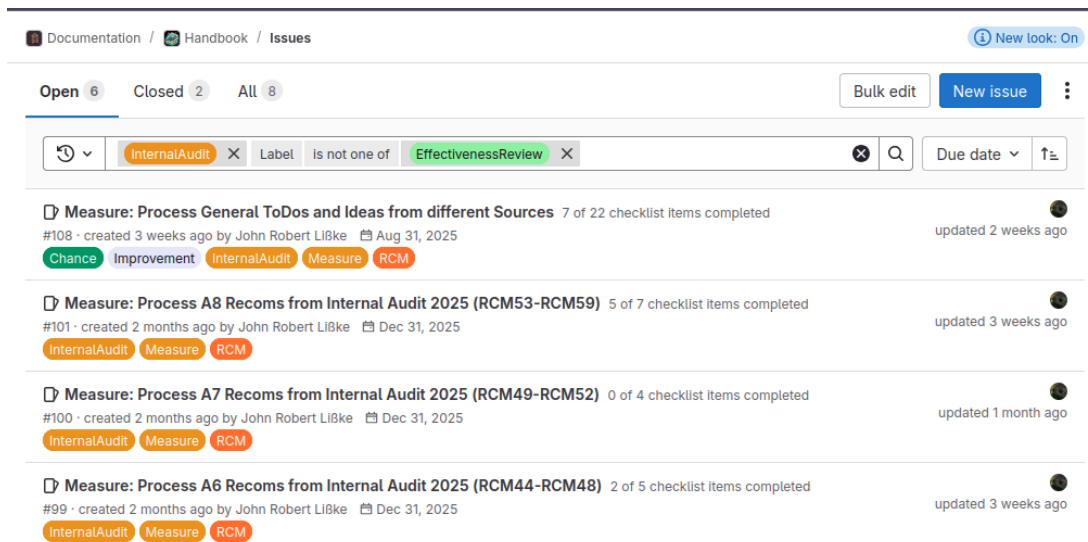


Figure 6: Using the Search Bar to Filter Issues by Tag

### 5.2.3 Board-Based Organization

To support visual tracking of dynamic ISMS processes, GitLab Issue Boards are used to group and manage tasks by category. Boards reflect key ISMS process areas, such as risk management, audits, or improvements. Columns are constructed based on GitLab's label system.

Each board consists of horizontally arranged columns, where each column corresponds to a specific label. Issues tagged with that label automatically appear in the respective column. Example configurations include:

- **Risk-related process flow:**
  - Risk
  - Treatment
  - Improvement
  - Chance
  - TToDo, TMaintain – Treatment-related tasks, categorized as pending actions (ToDo) or ongoing maintenance (Maintain)
  - Effectiveness Review
- **Audit-related classification:**
  - NCA – Major Non-Conformity
  - NCB – Minor Non-Conformity
  - RCM – Recommendation / OFI

GitLab's interface supports:

- Drag-and-drop column ordering
- Manual prioritization of Issues within columns

- Advanced filtering by label, assignee, milestone, or due date

This lightweight Kanban-style approach enhances visibility, prioritization, and progress tracking—ideal for maintaining audit readiness with minimal administrative burden.

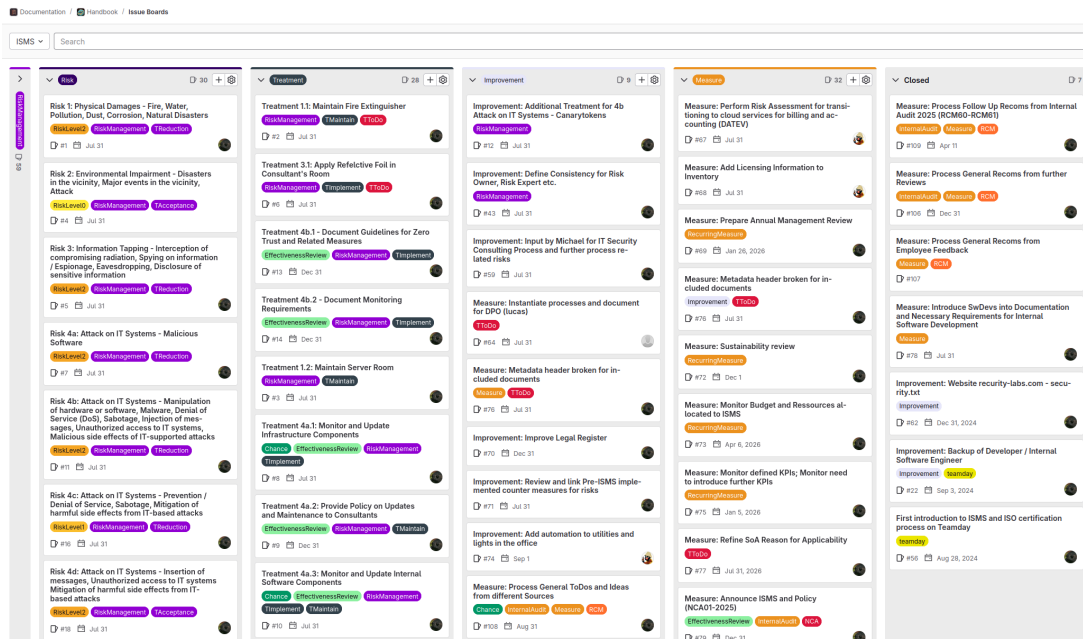


Figure 7: Risk Issue Board

### 5.2.4 Issue Templates

To standardize Issue creation and ensure quality across recurring ISMS tasks, several GitLab Issue templates were developed and stored in `.gitlab/Issue_templates/`. When creating new Issues in GitLab, users can directly select from these templates to ensure consistent structure.

Each template provides a standardized framework for:

- **Required fields:**  
Core content such as Description, Root Cause Analysis, Source, and Measure Owner.
- **Optional checklists:**  
Follow-up items such as Documentation Update, Effectiveness Review, or linked supporting evidence.
- **Linked references:**  
While not enforced through the template syntax itself, GitLab's native linking allows connections between related Issues—e.g., linking a Treatment to its

corresponding **Risk**, or a **Measure** derived from an audit finding to the respective **Audit planning Issue**.

Templates cover a range of practical use cases, including:

- General and contextualized **risk reporting**
- **G0-threat** related baseline risks
- **Risk treatment** implementation
- **Measures**, such as actions identified from audit results

New templates are added on an as-needed basis throughout the lifetime of the ISMS, as additional use cases or recurring activities requiring standardization emerge.

Complete examples of the templates are provided in:

- Section 8.1.1 – Risk Assessment Template
- Section 8.1.2 – Risk Treatment Template
- Section 8.1.3 – General Measure Template

### 5.2.5 Real-World Examples

Typical living Issues in the GitLab-based ISMS include:

- **Risk Assessments:** Documented risks capturing threat sources, impact, mitigation strategies, and linked controls.
- **Audit Findings:** Non-conformities or recommendations categorized by severity, with assigned remediation tasks and accountable owners.
- **Improvement Suggestions:** Proposed changes or optimizations tracked with implementation reviews. These are often created in free-text format to simplify feedback collection from employees and encourage continuous input.
- **Topic-Specific Planners:** Issues created for recurring or ad-hoc tasks that are not directly derived from formal templates—for example, reminders to renew supplier contracts under ISO 27002 Clause 5.19.

Complete examples of these living artifacts are provided in the Appendix:

- Section 8.2.1 – Risk Assessment Example
- Section 8.2.2 – Audit Finding Example
- Section 8.2.3 – Improvement Suggestion Example
- Section 8.2.4 – Topic-Specific Issue Example

## 5.3 Integration of Tooling and Workflow

The Git- and GitLab-based ISMS is deeply embedded into the company's daily workflows, minimizing friction while ensuring clear accountability and structured collaboration.

### 5.3.1 Workflow Integration

Updates to ISMS documentation follow a standard Git workflow:

- Changes are committed in dedicated branches or private forks
- Merge Requests (MRs) are used to review and approve modifications
- Commit signing and optional MR approval rules support traceability and authorization

This process ensures that even minor policy changes or risk updates are visible, reviewable, and documented over time—aligning with ISO/IEC 27001's traceability and evidence requirements.

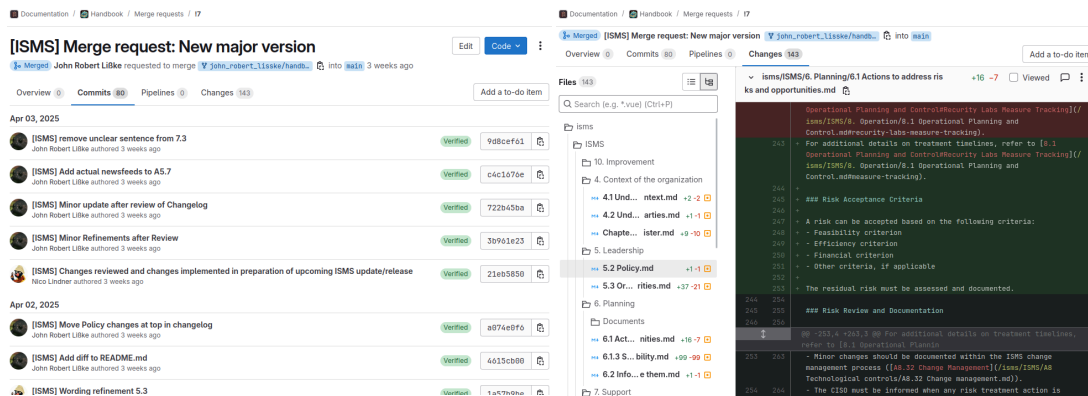


Figure 8: GitLab Commit History (left) and File Difference View (right) of a Merge Request

### 5.3.2 Seamless Fit into Daily Operations

The ISMS is designed to operate transparently in the background of daily routines:

- Issues for periodic reviews or audits appear like tasks in any other GitLab project
- Risks and improvements are logged as needed and integrated into general workflows
- The system encourages asynchronous collaboration, suitable for distributed teams

This helps normalize ISMS maintenance and avoids overhead caused by isolated tools or processes.

### 5.3.3 Tool Adoption Across User Types

While technical team members often interact with Git via Integrated Development Environment (IDE) or CLI integrations, non-technical staff primarily use the GitLab Web User Interface (UI). This lowers the barrier for participation and eliminates the need for training in Git internals.

The Web UI supports key ISMS activities, including:

- Editing Markdown documentation directly within the browser
- Creating *diffs* between commits
- Creating and managing Issues
- Applying predefined templates for structured tasks, such as audit tracking

Both usage patterns—CLI for technical users and Web UI for non-technical users—coexist seamlessly. This flexibility enables broader team participation, ensuring that all roles can contribute effectively according to their technical confidence and familiarity.

## 5.4 Internal and External Audit Execution

To evaluate the effectiveness and compliance of the implemented ISMS, both internal and external audits are systematically integrated into the process model. These audits assess conformity with ISO/IEC 27001 and validate whether the tooling and workflows support a traceable and continuously improving management system.

### 5.4.1 Internal Audit Process

Internal audits are conducted using the GitLab-based Issue system, allowing structured documentation, classification, and lifecycle tracking of findings. Each internal audit typically covers all ISO/IEC 27001 clauses and applicable *Annex A* controls.

- Findings are recorded using predefined Issue templates and classified with labels (e.g., NCB, RCM, Effectiveness Review)
- Responsibilities for remediation are assigned directly in the Issue (see Section 8.2.2), and corrective actions are tracked as linked follow-up Issues

This integration ensures that audit results are not only documented but actively managed and resolved within the operational ISMS environment.

### 5.4.2 Handling of Non-Conformities and Recommendations

Audit findings are immediately incorporated into the ISMS lifecycle:

- Non-Conformities differentiate between *Major Non-Conformities* (NCA ) and *Minor Non-Conformities* (NCB), documented as **Measure** Issues, assigned to specific owners, labeled appropriately, and scheduled with due dates
- Recommendations (RCM) are evaluated during audit follow-ups and, if accepted, converted into structured **Improvement** Issues
- Effectiveness reviews and corrective measures are monitored through labels, GitLab boards, and scheduled reviews

This structured handling ensures full traceability of Issues from identification through remediation and effectiveness verification.

### 5.4.3 External Audit Process (Certification Audit)

External certification audits are supported by the same GitLab-based documentation and Issue tracking infrastructure. Auditors are provided with selected files, logs, and process evidence as requested during the audit process.

- Documentation is presented in Markdown format, including full version histories and change tracking
- Live demonstrations of ISMS activity (e.g., open risks, treatments, audit findings) are performed using GitLab Issues and Boards
- No additional tooling beyond GitLab’s native features is required for audit support

This approach provides transparency, traceability, and efficiency—aligning closely with ISO/IEC 27001 certification expectations.

### 5.4.4 Management Review

In accordance with ISO/IEC 27001 Clause 9.3 [3], management reviews are conducted periodically—typically at least once per year—as part of ISMS performance evaluation. These reviews address:

- Evaluation of internal and external audit findings and their remediation status
- Assessment of ISMS objectives and associated key performance indicators (KPIs)
- Review of the effectiveness of implemented controls and improvement measures
- Consideration of changes in organizational context, the risk landscape, or business requirements
- Identification of resource needs and strategic improvement opportunities



Management review outcomes are documented and tracked within GitLab, using structured Issues or checklists linked to specific findings or action items. Follow-up actions are processed through the same traceable workflows applied to audit findings, ensuring seamless integration and accountability.

### **5.4.5 Post-Audit and Review Integration**

Audit findings and management review results are fully integrated into the living ISMS process:

- Issues are labeled, assigned priorities, and monitored until completion
- GitLab Boards provide visual overviews of open risks, non-conformities, and ongoing improvements
- Dedicated effectiveness reviews verify that implemented measures achieve the intended outcomes over time

This continuous feedback and action loop ensures that audits and reviews serve as operational tools for system maturity—rather than as isolated or purely formal reporting exercises.

The experiences gathered during implementation, internal and external audits, and management reviews form the foundation for the lessons learned, audit insights, and transferable recommendations presented in the following chapter (Section 6).

## 6 Lessons Learned, Audit Insights and Transferable Recommendations

This chapter reflects on the practical implementation of the Git- and GitLab-based ISMS, highlighting key lessons learned, insights gained from internal and external audits, and recommendations that can support other SMEs facing similar challenges.

### 6.1 General Feedback on the Use of Git

A key lesson learned during the development of the ISMS was the significant value of building on an existing, interactive collaboration model. Throughout the project, the involved parties worked in a highly iterative manner, engaging in continuous cycles of content creation and review. This dynamic exchange strengthened both the technical accuracy and the strategic alignment of the ISMS documentation.

The use of Git as a VCS proved to be a decisive factor in the success of this collaborative process. It enabled precise tracking of every change, making the evolution of each document transparent and easy to follow. Reviewing and commenting on individual *diffs* allowed contributors to focus on relevant updates without needing to re-read entire files—saving time and reducing review fatigue.

By providing a clear audit trail for every decision and modification, the Git-based workflow also fostered transparency and accountability. This approach not only improved the efficiency of internal reviews but also positioned the organization strongly for external audits, where the ability to demonstrate controlled, well-documented change management is a critical success factor.

Overall, the Git-driven review model emerged as a best practice for the company. It improved the quality, efficiency, and auditability of ISMS development and serves as a transferable pattern for other organizations aiming to implement governance and compliance processes with limited resources.

## **6.2 Applicability of the Process Model**

Based on the implementation experience, the PDCA cycle has proven to be an effective structuring framework for ISMS development—even within small IT security consulting companies. Its iterative nature supports incremental improvement, adaptability, and aligns well with ISO/IEC 27001’s emphasis on continual performance evaluation.

The file-based mapping of ISO clauses and controls to dedicated Markdown files further supports a modular and maintainable documentation approach. It provides clear traceability between requirements, implementation measures, and audit evidence. This modular structure facilitates targeted policy reviews, control assessments, and efficient audit preparation—especially in resource-constrained SME environments.

## **6.3 Feasibility of the Reference Implementation**

This section evaluates the practical feasibility of the Git- and GitLab-based ISMS, reflecting on key operational challenges and the structural adaptations made during implementation.

The Git-based ISMS model implemented in this thesis demonstrates that even highly resource-constrained organizations can maintain an ISO-compliant management system—provided the tools and processes are well-aligned with existing workflows.

### **6.3.1 Documentation and Policy Consolidation**

Generating policies directly from ISO control requirements initially proved to be error-prone, as it required manual synthesis and interpretation. Over time, the structure evolved into a hybrid model: reusable Markdown includes were combined with carefully curated standalone policy files.

This approach balances consistency with clarity and enables selective reuse of content across different parts of the ISMS, improving maintainability and auditability without sacrificing readability.

### **6.3.2 Access Control and Separation of Sensitive Areas**

While most ISMS documentation is accessible to all employees, sensitive components—such as incident reports, and supplier documentation—require restricted access. To address this, a separate GitLab namespace was introduced for confidential materials, including business continuity plans and incident handling.

This separation ensures that key ISMS objectives—protecting customer data, maintaining business continuity, and enabling compliance and transparency—are upheld, avoiding oversharing while supporting efficient collaboration within authorized teams.

### **6.3.3 Recurring Tasks and Process Maintenance**

Although the Git- and GitLab-based setup minimizes technical infrastructure overhead, the operational workload should not be underestimated. Key recurring tasks—such as annual reviews, recurring employee trainings, audit preparations, and regular policy updates—must be proactively scheduled and tracked.

GitLab Issues with labels and due dates proved effective in managing this workload, but only when supported by consistent ownership and documentation discipline. Without clear assignment of responsibilities, recurring tasks risk falling through the cracks over time.

## **6.4 Audit Insights**

To evaluate both compliance and operational effectiveness, the ISMS implementation was subjected to an internal audit and an external certification audit. The findings from these assessments provided critical feedback for improvement and confirmed the feasibility of the lightweight, Git-based approach.

### **6.4.1 Internal Audit**

The internal audit identified a range of findings, including:

- Missing or undocumented control implementations
- Undefined review cycles and unclear role responsibilities
- Incomplete traceability between risks and mitigation actions

Most findings were categorized as **Minor Non-Conformities** or **Recommendations (RCMs)**. Rather than exposing fundamental flaws, these issues reflected an early-stage maturity level typical of newly established management systems.

The audit process itself proved valuable for structuring improvements, clarifying responsibilities, and strengthening overall process discipline.

### **6.4.2 External Certification Audit**

The external certification audit concluded without identifying any major or minor non-conformities. Certification according to ISO/IEC 27001:2022 was successfully granted.

These results demonstrate that even a lean, Git-based ISMS—without enterprise-grade tools—can fully satisfy the requirements for certification when processes are clearly defined, actively maintained, and transparently documented.

## **6.5 Transferable Recommendations for Similar SMEs**

Based on the implementation experience and audit feedback, several key recommendations can be made for other SMEs considering a similar Git-based ISMS model:

- Use version-controlled, file-based documentation:  
Modular files aligned with ISO clauses enhance transparency, maintainability, and auditability.
- Manage living processes through Issues or similar ticketing systems:  
Track risks, treatments, audits, and improvements systematically through structured templates, labels, and boards.
- Define clear documentation practices for Issues:  
Since GitLab Issues are not version-controlled like repository files, important updates to risks, audits, or improvements should be recorded transparently in Issue comments or changelogs.
- Implement role-based access control:  
Separate sensitive information into protected namespaces or repositories while maintaining general ISMS visibility for all employees.
- Enforce repository discipline:  
In GitLab CE, fine-grained file ownership cannot be enforced natively. Organizational measures—such as contributor guidelines and mandatory review workflows—are necessary to maintain repository integrity.
- Carefully structure foundational policies early:  
Key policies such as the Information Security Policy (Clause 5.2) should be drafted as standalone documents from the outset to avoid later complexity due to fragmented or overextended includes.
- Consider Markdown compatibility:  
GitLab-specific features (such as includes) improve modularity in the web interface but may impact offline readability. If local access is needed, consider generating flattened versions or documenting limitations for readers.

- Avoid overengineering:

Focus on fulfilling core ISO requirements initially, and allow the ISMS to evolve based on audit results, operational feedback, and maturing needs.

- Assign clear ownership for recurring tasks:

Even small teams should designate responsible roles for activities such as audits, reviews, policy updates, and awareness trainings.

This approach enables technically skilled SMEs to establish and maintain an ISO-compliant, transparent, and sustainable ISMS with minimal overhead—while remaining flexible, scalable, and responsive to evolving security and business requirements.

## 7 Conclusion

This thesis developed and validated a framework and reference implementation for an ISMS tailored to the specific requirements of small IT security consulting organizations. The primary objective was to design a practical, scalable, and ISO/IEC 27001:2022-compliant solution that minimizes operational overhead while ensuring transparency, traceability, and continuous improvement.

To achieve this, a Git- and GitLab-based implementation was constructed, leveraging existing workflows for both static documentation and dynamic ISMS process management. ISO clauses and controls were mapped to modular Markdown files, while recurring activities such as risk assessments, audits, and improvements were operationalized using structured GitLab Issues.

The implementation followed the Plan-Do-Check-Act (PDCA) cycle, providing a structured methodology for establishing and continuously refining the system. Internal and external audits, including successful ISO/IEC 27001:2022 certification without major or minor non-conformities, confirm the system's effectiveness and practical viability.

Key contributions of this work include:

- A modular documentation structure that enhances clarity, maintainability, and auditability
- A fully integrated task and process management system using open-source tools
- Validation that full ISO compliance is achievable without enterprise-scale ISMS platforms

The findings demonstrate that technically oriented SMEs with limited administrative capacity can establish and sustain a certified ISMS by aligning tools and processes with their existing technical culture. The Git- and GitLab-based approach offers a transparent, cost-efficient, and sustainable alternative to traditional ISMS implementations.

This work contributes to the broader body of knowledge on lightweight ISMS architectures for SMEs and offers a transferable model for similar organizations. Future extensions may include the integration of automated reporting, risk visu-

alization, or adaptation to related fields such as software development firms or managed service providers.

In conclusion, the thesis shows that a structured yet lightweight ISMS implementation is not only feasible but highly effective in the SME context, provided that internal ownership, disciplined process modeling, and appropriate tooling are consistently applied.



## 8 Appendix

The following appendix provides supplementary material referenced throughout the thesis. It includes:

- Selected templates used for ISMS risk and measure management,
- Real-world examples illustrating the practical implementation,
- Acknowledgments regarding the development and review contributions.

These elements are intended to offer additional transparency into the operational aspects of the Git- and GitLab-based ISMS solution.

### 8.1 Examples from Issue Templates

The following subsections present real-world templates listed in Section 5.2.4.

#### 8.1.1 Risk Assessment Template

This template is used during the initial risk identification phase, especially for documenting baseline risks based on BSI G0 threat catalogs.

The G0-risk template is stored as a markdown file as follows:

1	Key	Value		markdown
2	-----	-----		
3	Process	General Operation		
4	Risk Expert	@john		
5	Process Owner	CEO		
6	Risk Owner	CEO		
7				
8	# Risk			
9	## Risk Identification			
10				
11	Key	Value		
12	-----	-----		
13	ID			
14	Aggregated Threat			

15	Covered BSI G0-Threats			
16				
17	<b>## Risk Analysis</b>			
18	Key	Value		
19	-----	-----		
20	Relevance	relevant		
21	Rationale for Relevance			
22	Implemented Counter Measures			
23				
24	<b>## Risk Assessment</b>			
25	Key	Value	Rationale	
26	-----	-----	-----	
27	Likelihood of Occurrence			
28	Damage Potential			
29	<b>**Risk Level**</b> [^1]		-	
30				
31	<b>## Risk Treatment</b>			
32				
33	- [ ] Avoidance			
34	- [ ] Reduction			
35	- [ ] Transfer			
36	- [ ] Acceptance			
37				
38	Treatment Measure	Issue ID	Status	
39	-----	-----	-----	
40				
41				
42	[^1]: Damage Potential x Likelihood of Occurrence			

A structured meta section complements the template, providing clear documentation directly within each GitLab Issue:

## Meta

### Risk Levels

Risk Value	Risk Treatment	Review of risk acceptance
1 - 2	These risks are generally accepted. However, the risk owner is free to further treat the risk using any of the other three methods.	Annual review
3 - 5	These risks should be treated through risk transfer, risk avoidance, or risk reduction. Written acceptance of the risk is only possible by the CISO or CEO of Recurity Labs.	Annual review
6 - 8	These risks should be treated through risk transfer, risk avoidance, or risk reduction. Written acceptance of the risk is only possible by the CEO of Recurity Labs.	Semi-annual review

2 >=10d or >=150k€	2	4	6	8
1 <=10d or <=150k€	1	2	3	4
DP / PO	1 less than every 10y	2 once in 2-10y	3 1-11 times a year	4 equal or more than 12 times a year

### Damage Potential

Nr.	Protection Need derived from Assessment	Damage Potential
1	Confidentiality	2
2	Integrity	2
3	Availability	2

### Likelihood of Occurrence

Level	Frequency
4	The incident occurs more than 12 times a year.
3	The incident occurs 1-11 times a year.
2	The incident occurs every 1 to 10 years.
1	The incident occurs less than once every 10 years.

Figure 9: Rendered Meta Section of G0 Risk Issue Template

8.1.2 Risk Treatment Template

This template is used during the treatment process for risks, specifically when the chosen risk treatment strategy is **Reduction**. It supports structured documentation of the implementation task and later evaluation of the effectiveness of the treatment.

The treatment template is stored as a Markdown file as follows:

1	Key	Value		markdown
2	-----	-----		
3	Risk ID			
4	Risk Description			
5	Risk Owner			
6	Treatment Measure Owner			
7	Effectiveness Review			
8	Status			
9				
10	# To Do / Deliverable (Treatment Measure and Explanation)			
11				
12				
13	# Effectiveness Review Result			

8.1.3 General Measure Template

This template is used across multiple ISMS processes where actions are required —such as implementing improvements, addressing audit findings, or executing corrective actions. It provides a consistent structure for planning, execution, and post-implementation review.

The measure template is stored as a Markdown file as follows:

1

	Key		Value	
2		-----		-----
3		Status		[Open; In Progress; Implemented; Discarded]
4		Source		
5		Measure Owner		
6		Effectiveness Review		
7				
8	# Measure Description			
9				
10	# Effectiveness Review Result			
11				
12	# Root Cause Analysis			
13				
14	> Only required if the source is one of the following:			
15	> - Major Non-Conformity (NCA) from Audit			
16	> - Minor Non-Conformity (NCB) from Audit			

markdown

### 8.2.1 Risk Assessment

## Risk 6e: Human Error - Disclosure of sensitive information - Leakage during communication with customers

Open

Issue created 7 months ago by John Robert Lißke

Key	Value
Process	IT Security Consulting
Risk Expert	@john_robert_lißke
Process Owner	OPS, CEO
Risk Owner	CEO

### Risk

#### Risk Identification

Key	Value
ID	6e
Threat	Human Error - Disclosure of sensitive information
Threat Details	Names of other customers or project names are "leaked" as part of customer communication (screen sharing/ account sharing)

#### Risk Analysis

Key	Value
Relevance	relevant
Rationale for Relevance	Some meetings require screen sharing Customers use same technology, e.g. SSO provider such as Microsoft/Azure
Implemented Counter Measures	

#### Risk Assessment

Key	Value	Rationale
Likelihood of Occurrence	3	Screen-sharing is sometimes requested or mandatory in meetings to discuss aspects of an assessment  Consultants have frequent project and customer changes (~2weeks/project)  Customers share technologies such as SSO of Microsoft that use confusing session management, which could lead to unintentional account linkings
Damage Potential	2	A customer noticing data of other customers during a meeting or assessment does not only set this data at risk for misuse, but can also be seen as a big reputation loss of RL as this looks like all customers data is at risk, also the data of the current customer.
Risk Level	6	-

#### Risk Treatment

☐ Avoidance

☒ Reduction

☐ Transfer

☐ Acceptance

The risk has to be further reduced by the following measure:

Treatment Measure	Issue ID
Treatment 6e.1: Implement Measures in guideline to prevent data leakage during projects	#55

Assignee

John Robert Lißke

Edit

Labels

Risk

RiskITSecurityConsulting

RiskLevel6

RiskManagement

TReduction

Dates

Start: None

Due: Jul 31, 2025

Milestone

None

Parent

None

Time tracking

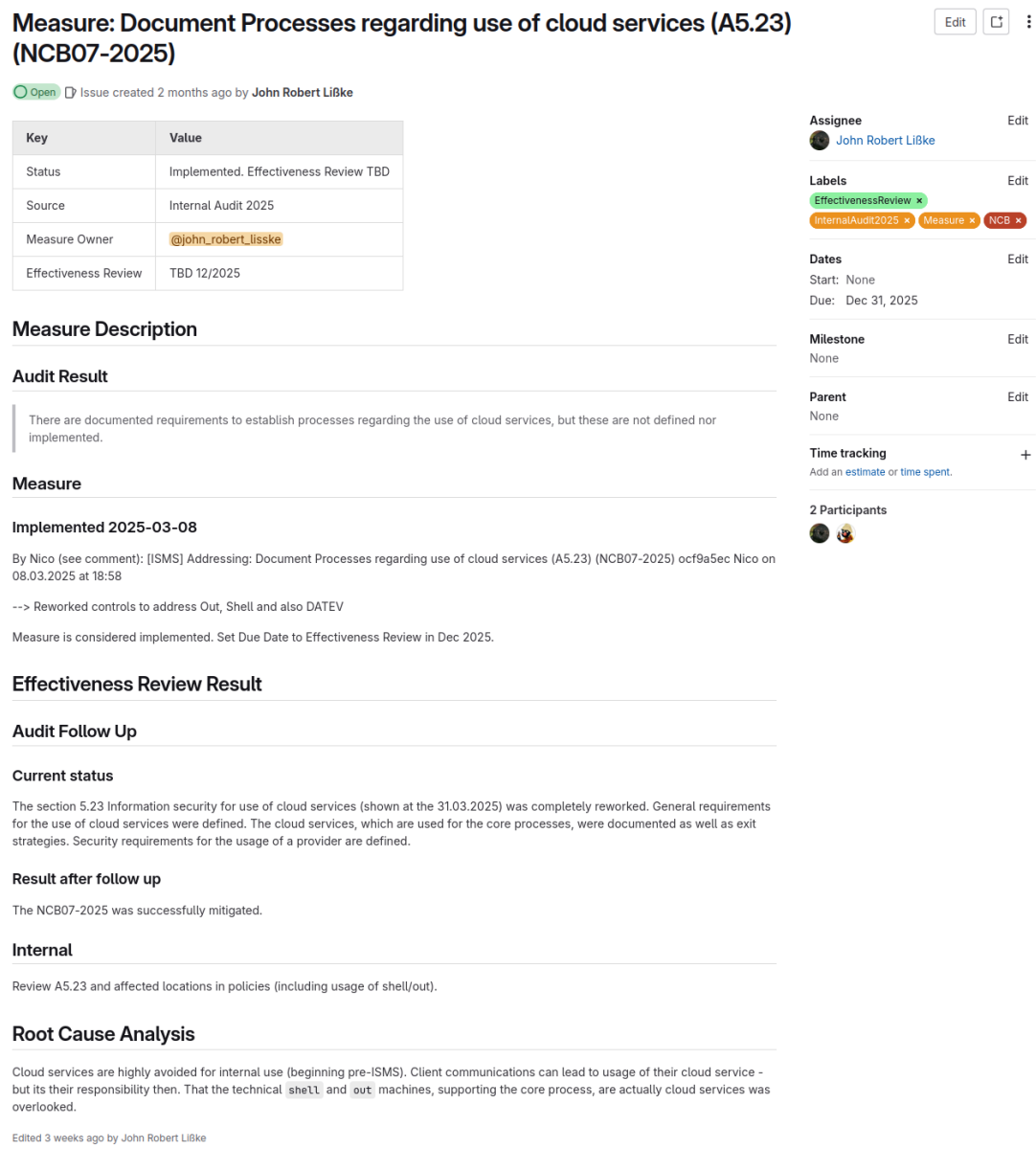
Add an estimate or time spent.

1 Participant

52

8.2.2 Audit Finding

The following figure illustrates a real-world example of a documented measure derived from an audit finding:



8.2.3 Improvement Suggestion

The following figure illustrates a real-world example of a documented freeform improvement suggestion:

Improvement: Website recurity-labs.com - security.txt

Closed

Issue created 7 months ago by John Robert Lißke

<https://www.rfc-editor.org/rfc/rfc9116>

discuss and consider to implement security.txt on our web page.

0

0

0

Add design

Child Items

Add

No child items are currently assigned. Use child items to break down work into smaller parts.

Linked Items

Add

Link items together to show that they're related or that one is blocking others.

Activity

All activityOldest first

John Robert Lißke changed due date to December 31, 2024 7 months ago

John Robert Lißke added Improvement label 7 months ago

John Robert Lißke assigned to @john 7 months ago

John Robert Lißke @john\_robert\_lasske · 4 months ago

Discussed with @lucas.

Creation of security.txt

Creation of security@recurity-labs.com

<https://recurity-labs.com/well-known/security.txt> created and linked in impress.

John Robert Lißke closed 4 months ago

Assignee

John Robert Lißke

Edit

Labels

Improvement

Edit

Dates

Start: None

Due: Dec 31, 2024

Edit

Milestone

None

Edit

Parent

None

Edit

Time tracking

Add an estimate or time spent.

+

1 Participant

Figure 12: Real-world Closed Improvement Suggestion



8.2.4 Topic-Specific Issues

The following figure illustrates a list of Issues created for tracking a specific ISMS-related task—in this case, NDA monitoring:

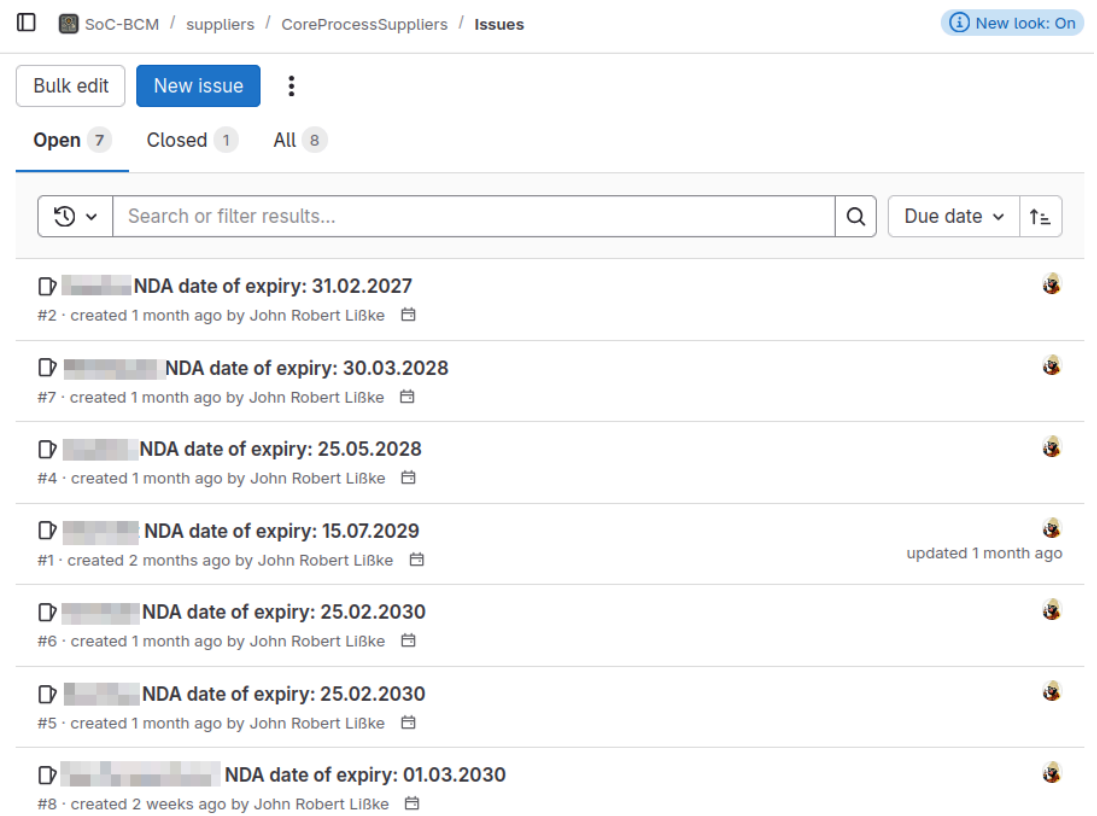


Figure 13: Real-world List of Topic-Specific Issues

### 8.3 Acknowledgment of Company Support

The development, implementation, and documentation of the ISMS described in this thesis were made possible through the trust and support of my colleagues at Recurity Labs and its leadership.

Special thanks go to Nico Lindner, who entrusted me with the responsibility of designing and operationalizing the ISMS, and who supported the necessary organizational changes and resource allocation throughout the project. In addition, Nico Lindner contributed to the final review (*Lektorat*) of the thesis, ensuring both technical accuracy and linguistic clarity. His involvement also ensured that all statements regarding the decision-making processes, company context, and implementation specifics were reviewed and confirmed from an organizational perspective.

This thesis reflects not only an academic investigation but also the result of a real-world collaboration within a technically driven and forward-thinking organization.

# Abbreviations

*CEO* – Chief Executive Officer

*CISO* – Chief Information Security Officer

*CLI* – Command Line Interface

*DSR* – Design Science Research

*HR* – Human Resources

*IDE* – Integrated Development Environment

*IEC* – International Electrotechnical Commission

*ISMS* – Information Security Management System

*ISO* – International Organization for Standardization

*ISRM* – Information Security Risk Management

*KPI* – Key Performance Indicator

*MR* – Merge Request

*OPI* – Opportunity for Improvement

*PDCA* – Plan-Do-Check-Act

*PGP* – Pretty Good Privacy

*RFC* – Request for Comment

*SME* – Small and Medium-sized Enterprise

*SoA* – Statement of Applicability

*SSH* – Secure SHell

*UI* – User Interface

*VCS* – Version Control System

# Bibliography

- [1] ISO/IEC, “ISMS – A Practical Guide for SMEs.” [Online]. Available: <https://www.iso.org/>
- [2] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design science in information systems research,” *MIS Q.*, vol. 28, no. 1, pp. 75–105, Mar. 2004.
- [3] ISO/IEC, *Information Security Management Systems – Requirements (ISO/IEC 27001:2022)*. International Organization for Standardization, 2022.
- [4] ISO/IEC, *Information Security Controls (ISO/IEC 27002:2022)*. International Organization for Standardization, 2022.
- [5] ISO/IEC, *Information Security Management System Implementation Guidance (ISO/IEC 27003:2017)*. International Organization for Standardization, 2017.
- [6] ISO/IEC, *Information Security Risk Management (ISO/IEC 27005:2018)*. International Organization for Standardization, 2018.
- [7] ISO/IEC, *Privacy Information Management (ISO/IEC 27701:2019)*. International Organization for Standardization, 2019.
- [8] D. Stelzer, *IT-Sicherheitsmanagement nach der neuen ISO 27001*. Springer Vieweg, 2020.
- [9] Bundesamt für Sicherheit in der Informationstechnik, “IT-Grundschutz-Kompendium 200-1: Managementsysteme für Informationssicherheit (ISMS),” 2022.
- [10] Bundesamt für Sicherheit in der Informationstechnik, “IT-Grundschutz-Kompendium 200-2: IT-Grundschutz-Methodik,” 2022.
- [11] Bundesamt für Sicherheit in der Informationstechnik, “IT-Grundschutz-Kompendium 200-3: Risikoanalyse auf der Basis von IT-Grundschutz,” 2022.
- [12] byght GmbH, “Einführung eines ISMS gemäß ISO 27001.” [Online]. Available: <https://www.byght.de/>

- [13] European Commission, “SME Definition – Internal Market, Industry, Entrepreneurship and SMEs.” [Online]. Available: [https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition\\_en](https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en)
- [14] Git Contributors, “Git – Distributed Version Control.” [Online]. Available: <https://git-scm.com/>
- [15] GitLab Inc., “GitLab Community Edition Licensing.” [Online]. Available: <https://docs.gitlab.com/ee/development/licensing/>

# List of Figures

Figure 1	Clause Structure of ISO/IEC 27001:2022 .....	5
Excerpt 1	ISMS Scope .....	12
Excerpt 2	ISMS Objectives of the Reference Implementation .....	13
Excerpt 3	Clause Mapping .....	16
Excerpt 4	ISMS Policies .....	17
Figure 2	File Tree - /isms .....	27
Figure 3	Structure - ISMS/Policies and ISMS/AX Policy Includes .....	28
Figure 4	Head of Exemplary Audit Issue .....	30
Figure 5	List of Labels for ISMS Issues .....	32
Figure 6	Using the Search Bar to Filter Issues by Tag .....	33
Figure 7	Risk Issue Board .....	34
Figure 8	GitLab Commit History (left) and File Difference View (right) of a Merge Request .....	36
Figure 9	Rendered Meta Section of G0 Risk Issue Template .....	49
Figure 10	Real-world Risk Assessment Example .....	52
Figure 11	Real-world Audit Measure Example .....	53
Figure 12	Real-world Closed Improvement Suggestion .....	54
Figure 13	Real-world List of Topic-Specific Issues .....	55

# Declaration of Independent Processing

## Eidesstattliche Erklärung

John Robert, Lißke, 904651

I hereby certify that I have written this thesis independently and have used no sources or aids other than those stated. All parts of the thesis that are taken either verbatim or in substance from publications or lectures by other authors are clearly identified as such. I consent to a plagiarism check.

This thesis has not been submitted to any other examination authority, nor has it been published previously.

Hiermit erkläre ich an Eides statt, dass ich diese Arbeit selbstständig abgefasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinne nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht. Ich bin mit einer Plagiatsprüfung einverstanden.

Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

<u>Guben</u>	<u>03.05.2025</u>	<u>John Robert Lißke</u>
Place / Ort	Date / Datum	Original Signature / Unterschrift