SaaS Provider – ISO 27001 Readiness Assessment
Project Type: ISO/IEC 27001:2022 Readiness Review and Remediation Planning
Industry: SaaS / Cloud-based Software
Role: GRC / Cybersecurity Governance Practitioner
Duration: 4–6 weeks

Note: This is a **simulated case study** I developed as part of my governance, risk and compliance (GRC) portfolio, based on a realistic mid-size SaaS organization preparing for ISO 27001 certification.

---

1. Executive Summary

A mid-size SaaS provider was preparing for an ISO/IEC 27001:2022 certification to strengthen customer trust and support enterprise sales. Security practices existed, but they were informal, inconsistent across teams, and not clearly mapped to ISO 27001 requirements.

In this project, I designed and executed an **ISO 27001 readiness assessment** that:

- Defined the **ISMS scope** around the SaaS platform, supporting infrastructure and key business functions
- Assessed current controls against **Annex A** and core ISO 27001 clauses
- Identified and prioritized **control gaps** and documentation weaknesses
- Produced a practical, phased **remediation roadmap** aligned to business priorities and available resources

The result was a clear view of where the organization stood against ISO 27001 and a realistic plan to close the most important gaps before engaging a certification body.

---

2. Context & Problem

The simulated organization had grown quickly and had:

- A working security culture in engineering and operations
- Some controls in place (backups, access controls, change management, incident handling)
- Customer questionnaires and security addendums in contracts

However, it faced several challenges:

- No formal **ISMS scope**—unclear what was “in” or “out” for ISO 27001
- Policies and procedures existed in silos and were not aligned to a single standard
- Controls were not consistently documented or **evidenced**
- Risk management activities were informal and not captured in a structured **risk register**
- Leadership wanted to pursue ISO 27001, but lacked a clear picture of readiness, effort and timelines

The objective of this project was to answer three simple questions:

1. Where are we today against ISO 27001?
2. What is missing or weak?
3. What should we do first to prepare for an external audit?

---

3. Objectives

I defined four main goals for the readiness review:

1. **Clarify Scope:** Define a realistic ISMS scope around the SaaS platform and supporting processes.
2. **Assess Controls:** Map existing controls and practices to ISO/IEC 27001:2022 requirements.
3. **Identify Gaps:** Document gaps in controls, documentation, governance and evidence.
4. **Plan Remediation:** Propose a phased remediation plan with priorities, owners and timelines.

---

4. Approach & Methodology

4.1 Scoping the ISMS

- Identified key **assets and areas** to be included in scope:
    - SaaS application and production environment
    - Supporting cloud infrastructure and CI/CD pipeline
    - Customer data handling and support processes
    - Relevant internal functions (e.g., IT, security, product, support)
- Documented:
    - **Scope statement** (what is included/excluded and why)
    - **Context of the organization** (internal and external issues affecting the ISMS)
    - Key **interested parties** and their expectations (customers, regulators, partners, staff)

This provided a clear boundary for the readiness assessment and eventual certification.

4.2 Information Assets & Classification (High-Level)

- Listed major **information assets** (customer data, system logs, source code, configuration data, internal documents).
- Grouped them into logical categories rather than individual items, to stay practical.
- Applied a simple classification approach (e.g., Public, Internal, Confidential, Restricted) to guide control expectations.

This ensured the assessment focused on protecting what truly mattered.

4.3 Control Mapping to ISO/IEC 27001:2022

- Reviewed existing policies, procedures, and practices, such as:
    - Access control and account management
    - Backup and recovery processes
    - Change management and deployment practices
    - Incident response steps
    - Vendor and third-party management
- Mapped these to:
    - Relevant **ISO 27001 clauses** (e.g., 4–10 for ISMS context, leadership, planning, support, operation, evaluation, improvement)
    - **Annex A** controls, grouped by theme (organizational, people, physical, technological)

Created a simple **control matrix** showing:

- ISO requirement / control
- Existing practice or document
- Status: Fully in place / Partially in place / Not in place
- Notes and evidence references

4.4 Gap Analysis

From the control matrix, I identified key types of gaps:

- **Documentation gaps:**
    - Policies existed in email or slides, but not as approved, version-controlled documents
    - Some procedures were tribal knowledge in engineering teams
- **Control gaps:**
    - Limited formal risk assessments and lack of structured risk register
    - Inconsistent access reviews for privileged accounts
    - No clear, tested process for supplier risk and ongoing monitoring
- **Evidence gaps:**
    - Activities were being done, but no clear way to **prove** them to an auditor (e.g., meeting minutes, logs, tickets).

Each gap was documented with:

- Description
- Related ISO clause / Annex A control

- Risk/impact (qualitative rating)
- Suggested remediation action

4.5 Remediation Planning & Prioritization

Designed a **phased remediation plan**:

- **Phase 1 – Foundations (High Priority)**
    - Formalize ISMS scope and key policies (information security policy, access control, incident management, backup, acceptable use).
    - Establish a basic **risk management process** and risk register.
    - Define roles and responsibilities for the ISMS (ISMS owner, control owners).
- **Phase 2 – Controls & Evidence**
    - Strengthen access control processes (e.g., joiner-mover-leaver, periodic access reviews).
    - Document and standardize backup, restore and testing routines.
    - Improve incident response documentation and logging, including post-incident reviews.
    - Introduce simple **metrics and reporting** for management review.
- **Phase 3 – Governance & Continuous Improvement**
    - Plan and perform internal audits on key areas.
    - Set up regular **management review** of the ISMS.
    - Tighten vendor and third-party risk practices to align with ISO requirements.
    - Prepare for external certification (pre-assessment, document pack, evidence mapping).

Each action item had:

- Priority (High, Medium, Low)
- Owner / team
- Suggested timeline (e.g., 0–3 months, 3–6 months)

---

5. Deliverables

This simulated readiness assessment produced:

1. **ISMS Scope & Context Document**
    - Scope statement, interested parties, and key internal/external issues.
2. **Information Asset & Classification Overview**

    - High-level asset categories and classification scheme.

3. **ISO 27001 Control Mapping Matrix**
    - Table showing existing controls vs. ISO/IEC 27001:2022 requirements and Annex A controls.
4. **Gap Analysis Report**
    - List of control, documentation and evidence gaps with associated risk/impact notes.
5. **Phased Remediation Roadmap**
    - Prioritized list of actions with owners, suggested timelines and dependencies.

---

6. Outcomes & Impact (Simulated)

In this simulated scenario, the assessment delivered:

- A clear, shared understanding of **where the organization stands** against ISO 27001.
- A prioritized view of:
    - Which controls and documents must be addressed **before** engaging a certification body
    - Which improvements are important but can follow later
- Better alignment between security, engineering and leadership:
    - Security conversations shifted from “we need ISO 27001” to
      “here are the top 10 things we need to fix or formalize to be ready.”
- A realistic expectation on timelines and effort, reducing the risk of:
    - Rushing into an audit unprepared
    - Over-committing to unrealistic deadlines

---

7. My Role & Contributions

In this simulated project, I:

- Defined the **ISMS scope** and documented organizational context and interested parties.
- Built the **control mapping matrix**, linking current practices to ISO 27001 and Annex A controls.
- Led the **gap analysis**, identifying missing or weak controls, documentation and evidence.
- Designed the **phased remediation roadmap**, balancing risk, business impact and effort.
- Summarized findings in a structured format suitable for leadership and future discussions with auditors or certification bodies.

---

8. Lessons Learned & Next Steps

Key lessons from this project:

- ISO 27001 readiness is less about perfection and more about **clarity, structure and evidence**.
- Many organizations are “doing” security, but not **documenting or proving** it.
- A realistic, scoped approach prevents ISO from feeling overwhelming or purely theoretical.

Logical next steps for this simulated SaaS provider would be to:

- Execute the **Phase 1 remediation actions** (scope, policies, risk register, roles).
- Establish a regular **risk review and management review cadence**.
- Begin preparing a **document and evidence pack** for pre-assessment with a certification body.