Maverick Gardner Information Technologies & Solutions Inc.
1260 Journey's End Circle, Unit 11
Newmarket, Ontario
L3Y 8Z7

ISO 27001:2022 Readiness Guide

A Practical Roadmap to Certification
Prepared by Maverick Gardner Information Technology & Solutions

1. Introduction

In a world where data drives every decision, information security has become a business necessity. The **ISO 27001:2022** standard provides a globally recognized framework for managing information security risks, ensuring confidentiality, integrity, and availability across your organization.

This guide helps you understand what ISO 27001 is, how it applies to your business, and how to prepare effectively for certification — whether you're starting from scratch or updating from a previous version.

2. What Is ISO 27001:2022?

ISO 27001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an **Information Security Management System (ISMS)**.

The **2022 revision** modernizes the standard to reflect new threats and technologies — including cloud services, hybrid work, and supply-chain risk.

Key Changes in the 2022 Update

- Controls streamlined from 114 → 93 and grouped into **4 themes:** Organizational, People, Physical, and Technological.
- New controls addressing:
    - Threat intelligence
    - Data masking & encryption
    - Cloud service security
    - ICT readiness for business continuity
    - Configuration management
    - Secure coding practices

3. Why Certification Matters

- **Customer Trust:** Demonstrates robust data protection and compliance.

- **Regulatory Alignment:** Supports privacy and security laws (PIPEDA, GDPR, NIST, CGP).
- **Competitive Advantage:** Often a requirement in RFPs, contracts, and supply chains.
- **Operational Efficiency:** Standardizes risk management and IT governance.

4. ISO 27001:2022 Framework Overview

The ISMS operates on the **Plan–Do–Check–Act (PDCA)** cycle:

Stage	Focus	Key Actions
Plan	Establish the ISMS	Define scope, policies, risk assessment, objectives
Do	Implement	Apply controls, assign responsibilities, deploy safeguards
Check	Monitor & Review	Conduct audits, analyze incidents, measure performance
Act	Improve	Correct issues, update controls, enhance processes

5. Step-by-Step Readiness Roadmap

Step 1: Define Context & Leadership Commitment

- Identify stakeholders, regulatory obligations, and business objectives.
- Assign an ISMS owner or compliance lead.
- Secure leadership endorsement and resources.

Step 2: Determine Scope of the ISMS

- Decide what information, systems, or departments fall under certification.
- Document boundaries (e.g., cloud environments, third-party vendors).

Step 3: Perform Risk Assessment

- Identify information assets and potential threats.
- Evaluate risks using likelihood × impact.
- Prioritize mitigation through risk treatment plans.

Step 4: Develop the Statement of Applicability (SoA)

- Map applicable Annex A controls (93 total).
- Document inclusion/exclusion rationale.

Step 5: Implement Controls & Supporting Policies

- Develop and deploy key policies:
    - Information Security Policy
    - Access Control Policy
    - Incident Response Procedure
    - Asset Management Policy
    - Business Continuity Plan
- Ensure user awareness and training.

Step 6: Conduct Internal Audit

- Validate compliance and control effectiveness.
- Identify non-conformities and corrective actions.

Step 7: Management Review

- Leadership evaluates audit results, risk posture, and continual improvement.

Step 8: Engage a Certification Body

- Select an accredited registrar.
- Undergo Stage 1 (document review) and Stage 2 (on-site or remote audit).
- Address findings for certification approval.

6. Common Readiness Gaps

Gap	Description	Solution
Incomplete risk assessment	Missing or outdated registers	Use standardized templates & periodic reviews
Weak documentation	Policies not version-controlled	Centralize documents with revision tracking

Gap	Description	Solution
Lack of awareness training	Users unaware of roles	Implement mandatory annual training
Vendor risk ignored	Third-party security unassessed	Conduct supplier evaluations & NDAs
No evidence logs	Auditors can't verify activity	Automate logging & audit trails

7. Tools and Templates

To simplify readiness, Maverick Gardner provides clients with access to:

- **ISMS Policy Templates**
  (Information Security, Asset Management, Access Control)
- **Risk Assessment Workbook**
  (Asset, Threat, Likelihood, Impact scoring)
- **Statement of Applicability Template**
  (Aligned to ISO 27001:2022 Annex A)
- **Internal Audit Checklist**
  (For Stage 1 and 2 preparation)
- **Incident Response Plan**
  (For Section A.5.24 compliance)

(All included in our Compliance-as-a-Service framework.)

8. Continual Improvement

Certification is not the finish line — it's a cycle of continual improvement.
Regular reviews, internal audits, and corrective actions help your ISMS evolve alongside technology and emerging threats.

9. How Maverick Gardner Can Help

Our **Compliance-as-a-Service** integrates policy, process, and technology to keep you audit-ready at all times.
We manage documentation, monitoring, and evidence collection so your team can focus on operations while staying compliant.

Contact us:
info@maverickgardner.com
647-484-6045
www.maverickgardner.com

Appendix A – ISO 27001:2022 Control Summary (Condensed)

Themes & Example Controls

- **Organizational (37 controls)** — policies, risk, supplier, project security.
- **People (8 controls)** — awareness, training, disciplinary measures.
- **Physical (14 controls)** — access, protection, monitoring, secure areas.
- **Technological (34 controls)** — configuration, backup, encryption, logging, malware defense.