ISO 27001 Readiness Checklist

Prepared by KTMC Global – Accredited Training & Management Consultants

Empowering Professionals. Transforming Organizations.

■ Introduction

ISO 27001 is the world’s leading standard for managing information security. If your organization is preparing for certification, this checklist will help you identify what’s in place, what’s missing, and where to focus next. Think of it as a health check for your Information Security Management System (ISMS). Work through each section, tick the boxes you can answer 'Yes' to, and highlight areas that still need work.

1. Understanding Your Organization

■ Have you identified the internal and external factors that could affect your information security?

■ Do you know who your stakeholders are (clients, regulators, employees, partners) and what they expect?

■ Have you defined the boundaries of your ISMS (which systems, people, locations are covered)?

■ *Tip: A well-defined scope makes the rest of your ISMS easier to manage and audit.*

2. Leadership & Commitment

■ Is top management actively supporting the ISMS implementation?

■ Has an information security policy been approved and communicated across the organization?

■ Are roles and responsibilities for information security clearly defined?

■ *Tip: Leadership buy-in is essential. Without it, your ISMS will struggle to succeed.*

3. Risk Assessment & Treatment

■ Have you identified potential risks to your information assets (data, systems, processes)?

■ Do you have a risk assessment methodology in place?

■ Have you created a risk treatment plan to reduce or eliminate risks?

■ *Tip: ISO 27001 requires a structured approach to risk, not just ad-hoc fixes.*

4. Policies, Procedures & Controls

■ Are security policies documented and communicated to all employees?

■ Have you defined clear procedures for handling sensitive information?

■ Are technical and organizational controls (like access controls, firewalls, backups) in place?

■ *Tip: Policies set direction, procedures provide detail, and controls make it all work.*

5. Training & Awareness

■ Are all employees trained on information security awareness?

■ Do employees understand their role in protecting data?

■ Are training records kept and updated regularly?

■ *Tip: People are your first line of defense — awareness reduces human error risks.*

■ Final Note

This checklist is a starting point. Regularly review and update your ISMS to stay compliant and resilient against new threats. For personalized training, gap analysis, and certification support, partner with KTMC Global – your trusted PECB-accredited training provider.

■ Ready to take the next step? Visit us at www.ktmcglobal.com or contact us at info@ktmcglobal.com.