ISO 27001

Implementation & Assessment Capabilities

Independent. Certification-Ready. Globally Recognised.

Cybernion

www.cybernion.com | info@cybernion.com

What is ISO 27001?

ISO/IEC 27001 is the international standard for an Information Security Management System (ISMS). It sets out the requirements for establishing, operating, and continually improving information security, with controls drawn from Annex A. Certification is issued by an accredited certification body following a two-stage audit.

Certification Requirement

Organisations must operate a documented ISMS and pass a Stage 1 and Stage 2 audit by an accredited certification body to achieve certification.

Certification runs on a three-year cycle with annual surveillance audits, and full recertification every three years.

1

A System, Not a Checklist

Certification assesses a working management system, not a one-off snapshot. Controls must be operating and improving.

2

Scope Defines Certification

Only the defined ISMS scope is certified. The whole organisation is not automatically covered.

3

Certified by Accredited Bodies

Certification is issued by accredited bodies. Advisors and implementers prepare you, they do not certify.

Why ISO 27001?

Compliance & Risk

Provides a structured, auditable framework for managing information security risk

Market Access

Frequently required in tenders, supplier due diligence, and enterprise contracts

Security Maturity

Structured uplift of Confidentiality, Integrity, and Availability

Competitive Advantage

Expected by enterprise and international customers as a baseline of trust

Credibility & Trust

Independently demonstrates commitment to protecting customer and business data

Our ISO 27001 Services

A holistic service across Advisory, Implementation, and Assessment with independence between implementation and audit roles.

ISO 27001 Advisory

- ISMS gap analysis
- Risk assessment methodology
- Statement of Applicability design
- Scope definition support
- Annex A control guidance

ISO 27001 Implementation

- Annex A control implementation
- Evidence collection & management
- Documentation (ISMS, SoA, policies)
- Staff training and awareness
- Internal audit and management review

ISO 27001 Assessment

- Internal and pre-certification audit
- Control testing & verification
- Risk analysis across the ISMS
- ISMS Assessment Report
- Statement of Applicability (SoA)

ISO 27001 Certification Journey

Four stages, sustained through annual surveillance audits and three-yearly recertification.

1 Plan & Prepare

- Define scope, objectives & timeline
- Identify key security personnel
- Establish communication process
- Review existing documentation

2 Scope Definition

- Map ISMS boundaries & data flows
- Identify information assets & risks
- Agree applicable Annex A controls
- Define evidence requirements

3 Assess

- Internal audit and testing
- Verification against Annex A
- Risk analysis across the ISMS
- Management review

4 Certify

- ISMS Assessment Report
- Statement of Applicability (SoA)
- Detailed findings & recommendations
- Pathway to certification audit

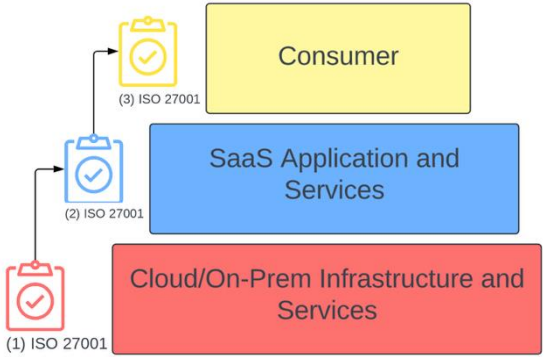
Case Study 1 - ISO 27001 Assessment

A growing SaaS provider engaged us to conduct a pre-certification assessment of its ISMS ahead of a Stage 2 audit, covering its AWS-hosted platform, corporate systems, and customer support operations.

Requirements

- Assess the effectiveness of Annex A controls implemented across the AWS platform and corporate systems against ISO 27001 requirements
- Assess the security of customer-facing support operations that handle personal and account data
- Provide recommendations to close gaps and improve readiness for the Stage 2 certification audit

Our Solution



By auditing the ISMS against Annex A and testing real controls, we gave the SaaS provider a clear view of its readiness and a prioritised set of actions to close before the certification audit.

Key Highlights

- **Plan and Prepare:** Define clear objectives, timeline, and comms process
- **Define the Scope:** Scope the assessment to cover the AWS platform, corporate systems, and support operations
- **Assess:** Conduct internal audit, control verification, and risk analysis across the ISMS
- **Report:** A detailed assessment report and control matrix highlighting strengths and gaps to close before Stage 2

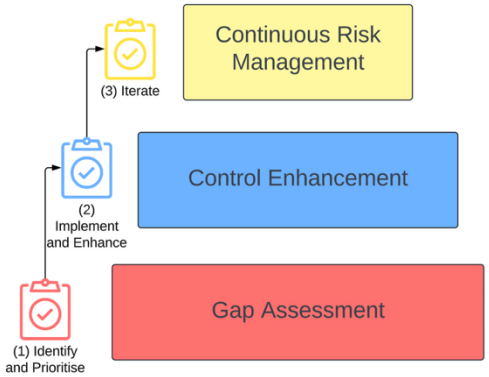
Case Study 1 - ISO 27001 Implementation

A professional services firm needed to establish an ISMS from the ground up to meet client contractual requirements and achieve ISO 27001 certification across its consulting and back-office functions.

Requirements

- Establish an ISMS aligned to ISO 27001 across consulting and back-office functions
- Implement Annex A controls to protect client and business information across systems and processes
- Prepare for Stage 1 and Stage 2 certification audits with robust, repeatable evidence
- Establish repeatable evidence collection and internal audit to sustain certification

Our Solution



A comprehensive gap analysis identified where practice fell short of ISO 27001, followed by control implementation, internal audit, and monitoring so the firm was fully prepared for certification.

Key Highlights

- **Gap Analysis:** A comprehensive assessment to identify gaps between current practice and ISO 27001 requirements
- **Control Implementation:** Design and implement Annex A controls across systems, people, and processes
- **Continuous Monitoring:** Internal audit and monitoring to sustain the ISMS and maintain certification
- **Documentation and Training:** Detailed ISMS documentation and staff training to support the new controls and audit

Important ISO 27001 Artefacts

The documents your auditor will examine, and what you receive in return.

Input: What You Provide

ISMS	ISMS Scope & Context
SoA	Statement of Applicability
RA	Risk Assessment
RTP	Risk Treatment Plan
ISP	Information Security Policy
IRP	Incident Response Plan
BCP	Business Continuity Plan
SOPs	Standard Operating Procedures
IAP	Internal Audit Programme
MRM	Management Review Minutes

+ Other policy and process documents as agreed during scoping.

Output: What You Receive

1 ISMS Assessment Report

A comprehensive evaluation of ISMS effectiveness against ISO 27001 and Annex A, covering identified risks, nonconformities, and their severity, with remediation guidance.

2 Statement of Applicability (SoA)

A structured mapping of Annex A controls showing which apply, their justification, and implementation status, forming the backbone of the certification audit.

Thank You

Ready to start your ISO 27001 journey? Let's talk.

Web www.cybernion.com

FAQs www.cybernion.com/insights

Email info@cybernion.com

Phone 0404 760 923

A Trusted Cyber Companion