ISO 27001 Readiness Checklist

ISO/IEC 27001:2022

Pera Prometheus
CONSULTING LTD ™
DEFENDING YOURINDUSTRY
Information Assured, Business Secured

How to use this checklist

- Work through each section. Tick items where you have evidence in place.
- Use the Status column to mark ✓ (done), × (gap) or — (not applicable with justification).

Organisation:

____

Date reviewed:

____

1 ISMS Foundation — Clauses 4–6

	Requirement	✓ / ×
■	Defined the scope of your ISMS (systems, data, locations and people)	
■	Documented an information security policy, signed off by senior leadership	
■	Identified internal and external issues relevant to information security	
■	Identified interested parties and their requirements (clients, regulators, supply chain)	
■	Set measurable information security objectives	

2 Risk Assessment & Treatment — Clause 6

	Requirement	✓ / ×
■	Documented a formal risk assessment methodology	
■	Completed a risk assessment covering all in-scope assets and processes	
■	Produced a risk treatment plan with named owners and target dates	
■	Completed a Statement of Applicability (SoA) covering all 93 Annex A controls	
■	Justified exclusions in the SoA with documented rationale	

3 Support — Clause 7

	Requirement	✓ / ×
■	Allocated sufficient resource and budget for ISMS operation	
■	Maintained records of security awareness training for all relevant staff	
■	Documented ISMS procedures are version-controlled and accessible to those who need them	

4 Operational Controls — Clause 8 & Annex A

	Requirement	✓ / ✗
■	Asset register maintained and kept current	
■	Access control policy in place; access rights reviewed at least annually	
■	Encryption policy documented and applied to sensitive data at rest and in transit	
■	Vulnerability management process in place; patches applied to a defined schedule	
■	Supplier security assessed and documented (cloud providers, subcontractors, IT vendors)	
■	Incident response plan documented, tested and assigned to named individuals	
■	Business continuity and disaster recovery plan in place and tested	

5 Performance, Internal Audit & Management Review — Clauses 9–10

	Requirement	✓ / ✗
■	Internal audit programme in place; at least one full audit cycle completed	
■	Audit findings documented with corrective actions and close-out evidence	
■	Management review conducted; minutes and action log maintained	
■	Nonconformities logged and tracked through to closure	

This checklist covers the mandatory requirements of ISO/IEC 27001:2022. It is intended as a readiness self-assessment tool, not a substitute for a formal certification audit.

Next Steps

What to do with your results

Gap Assessment Map your controls against all 93 Annex A requirements. Produce a prioritised remediation plan.	**ISMS Build** Document policies, assign control owners, complete risk assessment and Statement of Applicability.	**Internal Audit** Full internal audit against all clauses. Raise and close nonconformities before the certification body arrives.	**Certification** Stage 1 reviews documentation. Stage 2 tests implementation against evidence. Certificate issued.
■ **4–6 weeks**	■ **8–16 weeks**	■ **4 weeks**	■ **6–8 weeks**

Ready for certification?

If you ticked every box with confidence and have evidence to support each item, you are in a strong position for Stage 1 audit.

Gaps identified?

Work through unchecked items in order of risk. Prioritise your risk treatment plan, SoA and supplier assessments — these are audited first.

Not sure where you stand?

A structured gap assessment will map your current controls against all 93 Annex A requirements and give you a prioritised remediation plan.

ISO 27001 Gap Assessment

A full gap analysis against ISO/IEC 27001:2022, mapped to all 93 controls. You receive a prioritised remediation plan, not a generic report.

ISMS Build & Implementation

Build your ISMS documentation, risk assessment, Statement of Applicability and control evidence — audit-ready, from the ground up.

Audit Readiness & Stage 2 Support

Pre-audit review, mock interviews and evidence checks so your team is prepared before the certification body arrives.

Book a Compliance Assessment

pera-prometheus.com/contact