INFORMATION SECURITY MANAGEMENT SYSTEM

ISO/IEC 27001:2022

Management Aide-Memoire

A PRACTICAL GUIDE TO BUILD, RUN AND OVERSEE YOUR ISMS

This single-page reference helps senior management understand what ISO 27001:2022 requires, the key areas you must oversee, and the evidence you should expect to see — so information security supports the organisation's objectives and protects customers, people and reputation.

7 Management clauses (4–10)	**93** Annex A controls
4 Control themes	**PDCA** Plan · Do · Check · Act
CIA triad Confidentiality · Integrity · Availability	Continual improvement

HOW TO USE THIS AIDE-MEMOIRE

- **The cycle** — how the ISMS runs as a continual Plan-Do-Check-Act loop (Clauses 4–10).
- **Coloured zones below** — each maps to a stage of the cycle: Plan · Do · Check · Act.
- **Oversight band** — the board's role and the questions to ask.

The ISMS Lifecycle — How the Standard Works

Clauses 4–10 · a continual Plan-Do-Check-Act cycle

PLAN Establish the ISMS | **DO** Operate | **CHECK** Evaluate | **ACT** Improve

1 CONTEXT 4.1–4.4
- Understand the organisation and its context
- Identify interested parties
- Define ISMS scope and boundaries

2 LEADERSHIP 5.1–5.3
- Leadership commitment
- ISMS policy
- Roles, responsibilities and authorities

3 PLANNING 6.1–6.2
- Risk assessment and treatment
- Legal and other requirements
- Security objectives and planning

4 SUPPORT 7.1–7.5
- Resources
- Competence
- Awareness
- Communication
- Documented information

5 OPERATION 8.1–8.3
- Implement and operate controls
- Manage changes
- Outsource securely

6 EVALUATE 9.1–9.3
- Monitor, measure, analyse and evaluate
- Internal audit
- Management review

7 IMPROVEMENT 10.1–10.2
- Nonconformity and corrective action
- Continual improvement
- Feed lessons back into the ISMS

CONTINUAL IMPROVEMENT — the cycle repeats: outputs from Improvement (Clause 10) feed back into Context (Clause 4)

Senior Management Oversight — Your Role

Governance wraps around the whole cycle

1 Set Direction — Approve the information security policy and strategic direction. Ensure security is everyone's responsibility.

2 Understand Risk — Review key risks to the business and challenge risk appetite and treatment decisions.

3 Provide Resources — Ensure adequate budget, people, skills, technology and time are available.

4 Monitor Performance — Review KPIs, incidents, audit results and supplier performance. Challenge underperformance.

5 Review & Approve — Review major plans, policies, changes and investments. Approve improvements and risk treatments.

6 Ensure Compliance — Ensure legal, regulatory and contractual obligations are met. Oversee breach notifications and reporting.

7 Respond to Issues — Ensure issues are escalated early and resolved. Make timely decisions on significant incidents.

8 Drive Improvement — Embed a culture of security, learning and continual improvement.

QUESTIONS SENIOR MANAGEMENT SHOULD REGULARLY ASK

1. What are the organisation's top information security and cyber risks, have any materially changed since the last review, and are any currently outside our agreed risk appetite?
2. What potentially high-impact security incidents, near misses, or control failures have occurred since the last review, and what assurance do we have that root causes have been addressed?
3. What emerging cyber threats or attack trends are currently affecting our sector, and what assurance do we have that our controls and response capabilities remain appropriate?
4. If the organisation experienced a significant cyber incident or ransomware attack today, how confident are we in our ability to detect, respond to, and recover critical operations within acceptable timeframes?
5. Have any critical vulnerabilities remained unresolved beyond approved remediation timelines, what residual risk does this create, and how many remediation targets have been missed?
6. Are there any material concerns regarding privileged access, leavers' access removal, third-party access, MFA coverage, or other key security controls across critical systems?
7. Where business, technology, supplier, or AI-related changes proceeded without formal security assurance involvement, what risks were accepted and by whom?
8. Which suppliers, outsourced services, or technology platforms currently present the greatest information security or operational resilience risk to the organisation?
9. Are there any unresolved high-risk audit findings, recurring control weaknesses, regulatory concerns, insurer issues, customer concerns, or overdue remediation actions?
10. What assurance do we have that staff behaviour, security culture, and the organisation's use of artificial intelligence remain appropriately governed, monitored, and compliant with our obligations?

BOARD FOCUS

What to watch now · cross-cutting

The handful of risks and indicators the board should actively track. Populate the placeholders with your organisation's current position.

Top Risks to Watch

Illustrative — replace with your current top risks

#	Risk	Owner	Status
1	**Ransomware & major disruption** — Could an attack halt critical operations? Test detection, response and recovery.	COO / CISO	To assess
2	**Third-party & supply chain** — A supplier or cloud provider breach can quickly become your breach.	Procurement / CISO	To assess
3	**Data breach & privacy** — Loss or exposure of personal and confidential data, and the regulatory fallout.	DPO / CISO	To assess
4	**Unpatched critical vulnerabilities** — Known, exploitable weaknesses left open beyond agreed remediation timelines.	IT / SecOps	To assess
5	**People & social engineering** — Phishing and credential theft remain the most common way in.	HR / CISO	To assess

KPIs the Board Should Watch

Set your own targets and current values

MFA coverage — Critical systems and users protected by multi-factor authentication. Target ≥ 99%	**Time to patch criticals** — Mean days to remediate critical vulnerabilities. Target ≤ 14d	**High risks overdue** — High/critical risks past their treatment due date. Target 0	**Awareness training** — Staff who completed mandatory security training. Target ≥ 95%
Phishing click rate — Staff clicking simulated phishing emails. Target ≤ 5%	**Audit actions on time** — Corrective actions (CAPA) closed by their due date. Target ≥ 90%	**Major incidents (12m)** — Significant security incidents in the last 12 months. Target · trend	**Critical suppliers assessed** — Key suppliers with a current security assessment. Target 100%

P — PLAN

Establish the ISMS · Clauses 4–7

Set context and leadership, assess risk, choose objectives and controls, and put the foundations and documentation in place.

Foundation Principles

What good looks like

- **RISK-BASED** — Focus on protecting what matters most to the organisation and its customers.
- **PROPORTIONATE** — Controls are appropriate to the size, use and complexity of the organisation.
- **INTEGRATED** — Information security is embedded in business processes and projects.
- **DOCUMENTED** — Keep suitable documented information to demonstrate conformance.
- **IMPROVE** — Use data, feedback and learning to strengthen the ISMS.

Documents You Must Have — At a Minimum

Core ISMS artefacts

- ✓ **Information Security Policy** — Approved by senior management.
- ✓ **Statement of Applicability** — Control selection, justification and owner.
- ✓ **Access Control Policy & Records**
- ✓ **KPIs & Reporting Dashboard**
- ✓ **ISMS Scope Statement** — Boundaries, locations, systems and services.
- ✓ **Information Security Objectives**
- ✓ **Awareness & Training Records**
- ✓ **Supplier & Cloud Risk Management**
- ✓ **Asset Register & Data Inventory**
- ✓ **Policies & Standards Suite** — Acceptable use, access, incident, remote, AI use.
- ✓ **Internal Audit Programme**
- ✓ **Business Continuity & DR Plans**
- ✓ **Risk Assessment & Treatment Plan** — Method, risks, likelihood, impact, actions.
- ✓ **Records Retention & Information Lifecycle**
- ✓ **Management Review Records**

D — DO

Operate the controls · Clause 8 + Annex A

Implement and run the 93 Annex A controls day-to-day, manage change and suppliers, and meet the organisation's operational obligations.

Annex A Control Themes — 93 Controls

Selected via the SoA in Plan, operated here in Do

Organisational — 37 controls · A.5

Governance, policies, supplier and incident management, and legal compliance.

- **Policies & organisation** — A.5.1–A.5.8 — Policies, roles & responsibilities, segregation of duties, threat intelligence, security in projects.
- **Asset & information management** — A.5.9–A.5.14 — Asset inventory, acceptable use, classification, labelling, information transfer.
- **Access control & identity** — A.5.15–A.5.18 — Access control, identity management, authentication information, access rights.
- **Supplier & cloud security** — A.5.19–A.5.23 — Supplier relationships & agreements, ICT supply chain, service monitoring, cloud services.
- **Incident management** — A.5.24–A.5.28 — Planning, assessment & decision, response, learning, evidence collection.
- **Continuity & resilience** — A.5.29–A.5.30 — Security during disruption, ICT readiness for business continuity.
- **Legal, compliance & records** — A.5.31–A.5.37 — Legal & regulatory requirements, IP rights, protection of records, privacy & PII, independent review.

People — 8 controls · A.6

Screening, awareness, conduct and the responsibilities of staff.

- **Before & during employment** — A.6.1–A.6.4 — Screening, terms & conditions, awareness & training, disciplinary process.
- **Change & confidentiality** — A.6.5–A.6.6 — Responsibilities after termination or change of role, confidentiality & NDAs.
- **Working practices** — A.6.7–A.6.8 — Remote working, information security event reporting.

Fewest controls, greatest exposure — people are the most common factor in security incidents.

Physical — 14 controls · A.7

Protecting premises, equipment, media and the working environment.

- **Secure areas** — A.7.1–A.7.4 — Security perimeters, physical entry, securing offices & facilities, physical monitoring.
- **Working environment** — A.7.5–A.7.7 — Protection from environmental threats, working in secure areas, clear desk & clear screen.
- **Equipment & media** — A.7.8–A.7.14 — Equipment siting, off-premises assets, storage media, utilities, cabling, maintenance, disposal.

Largely the same controls whether the office is organisation-owned or a serviced/hybrid workspace.

Technological — 34 controls · A.8

Technical controls across systems, applications, data and networks.

- **Endpoints & access** — A.8.1–A.8.5 — User endpoints, privileged access, access restriction, source-code access, secure authentication.
- **Capacity, malware & vulnerabilities** — A.8.6–A.8.8 — Capacity management, malware protection, technical vulnerability management.
- **Configuration & data protection** — A.8.9–A.8.12 — Configuration management, information deletion, data masking, data leakage prevention.
- **Backup, logging & operations** — A.8.13–A.8.19 — Backup, redundancy, logging, monitoring, clock sync, privileged utilities, software installation.
- **Network security & cryptography** — A.8.20–A.8.24 — Network security & services, segregation, web filtering, use of cryptography.
- **Secure development** — A.8.25–A.8.34 — Secure development lifecycle, application security, secure coding, testing, change management.

Legal, Regulatory & Contractual Obligations

Operational compliance · A.5.31–A.5.34

- **Confidentiality** — Protect confidential, customer and personal information at all times.
- **Data protection & privacy** — Comply with all data protection and privacy laws applicable in the regions where you operate.
- **Regulatory duties** — Meet your sector regulator, industry codes and certification requirements.
- **Contracts & obligations** — Meet customer, insurer and supplier security requirements.
- **Incident reporting** — Report serious breaches to regulators, insurers and affected parties within required timeframes.

C — CHECK

Monitor & evaluate · Clause 9

Confirm what must be in place and the evidence to expect; monitor, audit and hold management reviews to test that the ISMS is working.

Key ISMS Areas — What Must Be in Place & How to Demonstrate It

Assurance & evidence

Area type: Management-system clauses · Higher-risk operational areas · People · Physical — **Status (RAG):** On track · Gaps / in progress · Needs attention · To assess

#	ISMS AREA	STATUS	OWNER	ISO	WHAT MUST BE IN PLACE	EVIDENCE TO EXPECT
1	**Leadership & Governance**	To assess	Board / CEO	5.1–5.3	Visible leadership, clear roles, accountability and approved policy.	Board minutes, policy, role descriptions.
2	**Risk Management**	To assess	CISO / Risk owner	6.1	Documented risk process, current risk register and treatment actions.	Risk reviews, KRIs, treatment plan.
3	**Statement of Applicability**	To assess	CISO / ISMS Manager	6.1.3	Annex A controls selected or excluded with justification.	Approved SoA and review history.
4	**Security Objectives**	To assess	CISO / Exec sponsor	6.2	Measurable objectives and plans to achieve them.	Objectives register, KPI dashboard.
5	**Policies & Acceptable Use**	To assess	CISO / ISMS Manager	A.5.1, A.5.10, A.5.12	Approved policies communicated to all relevant people.	Policy documents and awareness records.
6	**Asset & Data Management**	To assess	IT / Information owners	A.5.9–A.5.14	Assets identified, owned and appropriately protected.	Asset register, classification, data map.
7	**Access Control & Identity**	To assess	IT / IAM team	A.5.15–A.5.18, A.8.2–A.8.5	Access based on need-to-know, MFA and access reviews.	Access reviews, leaver tickets, MFA reports.
8	**Supplier & Cloud Security**	To assess	Procurement / CISO	A.5.19–A.5.23	Suppliers and cloud services assessed, contracted and monitored.	Due diligence, DPAs, SLAs, reviews.
9	**Incident Management**	To assess	CISO / SecOps	A.5.24–A.5.28	Prepared to detect, respond, learn and report incidents.	Incident logs, playbooks, lessons learned.
10	**Business Continuity & ICT Resilience**	To assess	COO / BCM lead	A.5.29, A.5.30, A.8.13, A.8.14	Continuity and recovery capability tested.	BCP/DR plans, restore evidence.
11	**HR & People Security**	To assess	HR	A.6.1–A.6.8	People are suitable, aware and follow security requirements.	Training, NDAs, leaver records.
12	**Physical Security**	To assess	Facilities / Office mgmt	A.7.1–A.7.14	Offices, people and equipment physically protected.	Access logs, CCTV, disposal records.
13	**Vulnerability & Patch Management**	To assess	IT / SecOps	A.8.8, A.8.9	Technical vulnerabilities identified and remediated.	Scans, patch reports, exceptions.
14	**Logging, Monitoring & Detection**	To assess	SecOps / SOC	A.8.15, A.8.16	Security events captured, monitored and reviewed.	SIEM/EDR reports, alert tickets.
15	**Data Protection & Privacy**	To assess	DPO / Legal	A.5.31–A.5.34, A.8.10–A.8.12	Personal data and confidential information protected.	DPIAs, RoPA, DLP alerts.
16	**Internal Audit**	To assess	Internal Audit	9.2	Planned internal audit programme with competent auditors.	Audit reports, CAPA tracker.

Management Review — What You Should Expect

Clause 9.3

Senior management must review the ISMS at planned intervals to confirm it remains suitable, adequate and effective. Each input below also shows which of the board's standing questions (above) it helps answer.

- **Performance vs objectives & KPIs** — Are we meeting our security objectives? Look for trends over time, not one-off snapshots. BOARD Q 1 5
- **Changes in context** — New activities, technologies, threats or regulations that shift the risk picture since last review. BOARD Q 3 7
- **Risks & treatment effectiveness** — Is the risk register current, and are treatments actually reducing risk to within appetite? BOARD Q 1 4 6
- **Incidents & lessons learned** — What went wrong, what we learned, and whether root causes are genuinely fixed. BOARD Q 2 4
- **Audit results & corrective actions** — Internal and external findings — and whether corrective actions are closing on time. BOARD Q 9
- **Resources, competence & awareness** — Do we have the people, skills, budget and training the ISMS needs to work? BOARD Q 10
- **Supplier, cloud & AI risk** — Third-party, cloud and emerging-tech exposure — including how AI is governed and used. BOARD Q 7 8 10
- **Actions, owners & evidence** — Every decision becomes an owned action with a deadline and proof of completion. BOARD Q 5 9

A — ACT

Improve · Clause 10

Classify findings, fix root causes, capture lessons and embed the culture and success factors that drive continual improvement.

Classification of Findings

MAJOR NONCONFORMITY
Control requirement not met and there is a significant risk to confidentiality, integrity or availability, or breach of legal or regulatory obligation.

MINOR NONCONFORMITY
Control requirement not fully met, or evidence of inconsistent implementation creating moderate risk or potential non-compliance.

OBSERVATION / GOOD PRACTICE
Opportunity to improve efficiency, effectiveness or reduce risk beyond the current requirements.

All Findings Should Include

- ✓ **Finding** — A clear, factual statement of what was observed — objective, not opinion.
- ✓ **Reference** — The exact clause, Annex A control or policy it relates to — keep it traceable.
- ✓ **Root cause** — Why it happened, not just what — so the same issue cannot recur.
- ✓ **Owner and due date** — A named person accountable, with a realistic deadline. No owner, no progress.
- ✓ **Evidence** — Objective proof: documents, records, logs, screenshots or interview notes.
- ✓ **Classification** — Major, minor or observation — sets the severity and how urgently to respond.
- ✓ **Corrective action** — The specific, agreed fix that closes the gap and prevents recurrence.
- ✓ **Verification of closure** — Independent confirmation the action worked and the issue is truly resolved.

Success Factors

What makes the ISMS stick

- **Leadership commitment** — Visible, active sponsorship from the top. Security is treated as a business priority, not quietly delegated to IT.
- **Clear accountability** — Named owners for the ISMS, each risk and each control. Everyone knows their responsibilities and what they answer for.
- **Engaged, aware people** — A strong security culture: staff are trained, alert to phishing and threats, and report concerns early without fear of blame.
- **Effective risk management** — Risks are identified, prioritised and treated in line with appetite — decisions are evidence-based and revisited as things change.
- **Good supplier management** — Third parties and cloud services are assessed, contracted and monitored. The supply chain is managed as part of your own risk.
- **Reliable reporting** — Timely, honest, meaningful information reaches decision-makers — both good and bad news surface early, backed by evidence.
- **Learn, improve & adapt** — Incidents, audits and near-misses become lessons. The ISMS keeps evolving with the threat landscape and the business.

Information security is not just an IT issue.
It enables the organisation to deliver trusted services, protect customers, protect people and maintain reputation.

Improvements feed back into Plan — the cycle begins again.

© 2026 **CyberSolace®**. All rights reserved. · cybersolace.co.uk