INFORMATION SECURITY MANAGEMENT

ISO 27001:2022 Explained — The Complete ISMS Implementation Guide

The full story in one PDF — what the standard requires, what changed in 2022, and how to implement it step by step.

INSIDE THIS TOOLKIT

- ISO 27001 requirements, clause by clause
- Risk assessment & SoA worked example
- Mandatory documentation checklist
- Post-implementation audit readiness guide
- Annex A controls list & the 2022 changes
- ISMS implementation roadmap
- Common implementation pitfalls
- Glossary of 30+ key ISMS terms

20	93	11	10
PAGES	ANNEX A CONTROLS	NEW CONTROLS 2022	ISMS CLAUSES

This guide is produced by **GSDC — Global Skill Development Council**, a globally recognised professional certification body. Whether you are implementing ISO 27001 for the first time, transitioning from the 2013 edition, or preparing your team for a certification audit, this guide gives you every clause, control, and implementation step in one place.

> **ISO/IEC 27001:2022** is the world's leading standard for Information Security Management Systems. The October 2022 revision introduced 11 new controls, merged 57 existing controls, and restructured Annex A from 114 controls across 14 domains into **93 controls across 4 themes**. All previously ISO 27001:2013-certified organisations had until **October 2025** to transition.

Table of Contents

ISO 27001:2022 Explained — The Complete ISMS Implementation Guide · 20 pages

How to use this guide: Implement teams should read cover-to-cover. Transitioning from 2013? Jump to Page 4. Preparing for audit? Focus on Pages 12, 15, and 17. The SoA worked example on Page 11 is the most-used section — bookmark it.

What is ISO 27001?

Standard overview, purpose, and the CIA triad at its core

ISO/IEC 27001 is the internationally recognised standard specifying requirements for establishing, implementing, maintaining and continually improving an **Information Security Management System (ISMS)**. It is jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Unlike prescriptive IT security standards, ISO 27001 is a **management system standard** — it does not mandate specific technology solutions. Instead it requires organisations to systematically identify their information security risks and implement appropriate, proportionate controls to manage those risks.

CIA	93	70K+
CONFIDENTIALITY · INTEGRITY · AVAILABILITY	ANNEX A CONTROLS (2022)	CERTIFIED ORGANISATIONS GLOBALLY

Core Principles

Principle	What it means	Example control
Confidentiality	Information accessible only to authorised individuals	Access control, encryption, NDA
Integrity	Information is accurate and protected from unauthorised alteration	Change control, digital signatures, audit logs
Availability	Information and systems accessible when needed by authorised users	Redundancy, DR/BCP, patch management

Why ISO 27001 Matters in 2026

1. **Regulatory alignment:** GDPR (EU), NIS2 Directive, DORA, UK Cyber Essentials Plus, and dozens of national cybersecurity laws reference ISO 27001 as a recognised compliance baseline.
2. **Supply chain mandates:** Fortune 500 enterprises, financial institutions, and government agencies now require ISO 27001 certification from suppliers before contract award.
3. **Breach cost reduction:** IBM's 2024 Cost of a Data Breach report found organisations with mature security practices — hallmarks of an ISMS — experienced breach costs 28% lower than average.
4. **Market differentiation:** For SaaS, cloud, and professional services firms, ISO 27001 certification shortens enterprise sales cycles and eliminates lengthy vendor security questionnaires.
5. **Cyber insurance:** Underwriters increasingly require evidence of an ISMS (not just a policy document) as a condition of cyber insurance cover and competitive premiums.

> **GSDC Note:** GSDC offers ISO 27001 Lead Auditor and Lead Implementer certifications that qualify professionals to design, implement, and audit ISMS programmes. See Page 18 for the full certification pathway.

What Changed in 2022

Full delta from ISO 27001:2013 — the changes every implementer must know

Structural Changes

Aspect	2013	2022
Annex A domains	14	4 themes
Total controls	114	93
New controls	—	11
Merged controls	—	24 merged
Revised controls	—	58 revised
Unchanged controls	—	11
Control attributes	None	5 per control

Clause Changes

Clause	Key change
4.2	New requirement: relevant interested party requirements that will be addressed via ISMS
6.1.3	SoA must now reference applicable controls from Annex A only
6.3	New clause: Planning of changes — formal change management for ISMS changes
8.1	Criteria for operational planning processes must now be documented
9.3	Management review inputs restructured into 9.3.1/9.3.2/9.3.3

The 11 New Annex A Controls (2022)

Control	Title	Theme
A.5.7	Threat intelligence	Organisational
A.5.23	Information security for use of cloud services	Organisational
A.5.29	Information security during disruption	Organisational
A.5.30	ICT readiness for business continuity	Organisational
A.6.7	Remote working	People
A.7.4	Physical security monitoring	Physical
A.8.9	Configuration management	Technological
A.8.10	Information deletion	Technological
A.8.11	Data masking	Technological
A.8.23	Web filtering	Technological
A.8.28	Secure coding	Technological

Clause-by-Clause Requirements: Clauses 4–6

Context, leadership, and planning — the foundational requirements of ISO 27001:2022

Clause 4 — Context of the Organisation

Foundational

- ✔ **4.1** Understanding the organisation and its context — identify internal and external issues that affect the ISMS
- ✔ **4.2** Understanding needs and expectations of interested parties — list parties, their requirements, and *(2022 update)* which requirements will be addressed by the ISMS
- ✔ **4.3** Determining the scope of the ISMS — document scope boundaries, locations, assets, exclusions with justification
- ✔ **4.4** ISMS — establish, implement, maintain, and continually improve the ISMS in accordance with the standard

Clause 5 — Leadership

Mandatory

- ✔ **5.1** Leadership and commitment — top management must demonstrate commitment through policy approval, resource allocation, and integration of ISMS into business processes
- ✔ **5.2** Policy — information security policy must be appropriate to purpose, include objectives, and be communicated and available to all relevant parties
- ✔ **5.3** Organisational roles, responsibilities and authorities — assign and communicate who is responsible for ISMS roles; top management must ensure ISMS reports on performance to them

Clause 6 — Planning

Critical — Risk Core

- ✔ **6.1.1** General — plan actions to address risks and opportunities; consider issues from 4.1 and requirements from 4.2
- ✔ **6.1.2** Information security risk assessment — define and apply a risk assessment process: establish criteria, identify risks, analyse and evaluate them; documented process required
- ✔ **6.1.3** Information security risk treatment — select appropriate treatment options; determine controls needed; produce SoA referencing all Annex A controls with applicability decisions and justifications
- ✔ **6.2** Information security objectives — establish measurable ISMS objectives at relevant functions and levels; plan how to achieve them
- ✔ **6.3** **NEW in 2022** — Planning of changes — when changes to the ISMS are needed, carry them out in a planned manner

Implementation tip — Clause 6.1.3 SoA: The Statement of Applicability is the single most scrutinised document in any ISO 27001 certification audit. It must list all 93 Annex A controls, state whether each is applicable or not, provide a justification for every exclusion, and cross-reference back to the risk treatment decisions that selected each included control.

Clause-by-Clause Requirements: Clauses 7–10

Support, operation, performance evaluation, and improvement

Clause 7 — Support

Operational Foundation

- **7.1** Resources — determine and provide the resources needed to establish, implement, maintain and improve the ISMS
- **7.2** Competence — determine required competence for ISMS roles; ensure people are competent via training or experience; retain evidence
- **7.3** Awareness — all persons doing work under the ISMS must be aware of the policy, their contribution, and implications of not conforming
- **7.4** Communication — determine internal and external communication needs: what, when, who, how
- **7.5** Documented information — create and update documented information; control its availability, suitability, and protection

Clause 8 — Operation

Execution

- **8.1** Operational planning and control — plan, implement, and control processes; *(2022 update)* criteria for processes must now be documented
- **8.2** Information security risk assessment — perform risk assessments at planned intervals or when significant changes occur; retain documented results
- **8.3** Information security risk treatment — implement the risk treatment plan; retain results as documented information

Clause 9 — Performance Evaluation

Measure & Monitor

- **9.1** Monitoring, measurement, analysis and evaluation — determine what to monitor, how to do it, when results are analysed, and who analyses them
- **9.2** Internal audit — establish, implement, and maintain an audit programme; auditors must be objective and impartial; retain results
- **9.3** Management review — *(2022 update)* now split into 9.3.1 (general), 9.3.2 (inputs), 9.3.3 (results); top management must review ISMS at planned intervals

Clause 10 — Improvement

Continual Improvement

- **10.1** *(2022 renumbered)* Continual improvement — continually improve the suitability, adequacy, and effectiveness of the ISMS
- **10.2** *(2022 renumbered)* Nonconformity and corrective action — when a nonconformity occurs: react, evaluate root cause, implement corrective action, review effectiveness, update risks, retain documented information

Annex A Controls — Theme 1: Organisational

A.5 — 37 controls covering policies, roles, asset management, supplier security, and incident management

About Annex A in 2022: Annex A now organises all controls into 4 themes (Organisational, People, Physical, Technological) replacing the 14 domains of the 2013 edition. Each control now carries 5 attributes: control type, information security properties, cybersecurity concepts, operational capabilities, and security domains — enabling easier filtering and mapping.

A.5.1 – A.5.5

Policies, Roles & Responsibilities

- → Information security policies (5.1)
- → Roles & responsibilities (5.2)
- → Segregation of duties (5.3)
- → Management responsibilities (5.4)
- → Contact with authorities & special groups (5.5–5.6)

A.5.7 NEW 2022

Threat Intelligence

- → Collect & analyse threat information
- → Relevant, insightful, contextual
- → Feed into risk assessment process
- → Share with stakeholders appropriately

A.5.8 – A.5.14

Project, Asset & Information Security

- → Information security in projects (5.8)
- → Inventory of information assets (5.9)
- → Acceptable use of assets (5.10)
- → Return of assets (5.11)
- → Classification & labelling (5.12–5.13)
- → Information transfer (5.14)

A.5.15 – A.5.19

Access Control & Authentication

- → Access control policy (5.15)
- → Identity management (5.16)
- → Authentication (5.17)
- → Access rights management (5.18)
- → Information security in supplier (5.19)

A.5.20 – A.5.22

Supplier & Service Provider Security

- → Addressing security in supplier agreements
- → ICT supply chain security management
- → Monitoring & reviewing supplier services
- → Changes to supplier services

A.5.23 NEW 2022

Cloud Services Security

- → Define cloud service acquisition criteria
- → Establish security requirements for cloud
- → Monitor cloud service compliance
- → Manage cloud exit / migration

A.5.24 – A.5.28

Incident Management

- → Incident management planning (5.24)
- → Assessment & decision on events (5.25)
- → Response to incidents (5.26)
- → Learning from incidents (5.27)
- → Collection of evidence (5.28)

A.5.29–5.37 2× NEW

BCM, Compliance & ISMS Review

- → Info security during disruption (5.29) *NEW*
- → ICT readiness for BCP (5.30) *NEW*
- → Legal & regulatory requirements (5.31–5.32)
- → IP rights & privacy (5.33–5.34)
- → Independent review of ISMS (5.35)
- → Compliance with policies (5.36)
- → Documented operating procedures (5.37)

Annex A Controls — Themes 2 & 3

A.6 People Controls (8 controls) · A.7 Physical Controls (14 controls)

Theme 2 — People Controls (A.6)

Human-element controls from pre-employment to termination

Control	Title	Key requirement
A.6.1	Screening	Background verification for all relevant personnel before or during employment, proportionate to role sensitivity
A.6.2	Terms and conditions of employment	Employment contracts must include information security responsibilities; signed prior to access being granted
A.6.3	Awareness, education and training	Regular, role-appropriate security awareness training; retain records of attendance and competency
A.6.4	Disciplinary process	Formal, communicated disciplinary process for information security policy violations
A.6.5	Responsibilities after termination	Information security responsibilities remain valid post-employment; access revoked promptly on leaving
A.6.6	Confidentiality or NDA agreements	Identify, document, and regularly review requirements for NDAs or confidentiality agreements
A.6.7	**Remote working** NEW 2022	Implement security measures for remote working; document policy covering BYOD, home networks, physical security of devices
A.6.8	Reporting information security events	Provide mechanism for staff to report events and weaknesses; ensure prompt, no-blame reporting culture

Theme 3 — Physical Controls (A.7)

14 controls protecting premises, equipment, and physical assets

Control	Title	Key requirement
A.7.1	Physical security perimeters	Define and use physical security perimeters to protect areas containing sensitive information
A.7.2	Physical entry	Secure areas protected by appropriate entry controls — only authorised personnel permitted
A.7.3	Securing offices, rooms, and facilities	Design and apply physical security for offices and facilities
A.7.4	**Physical security monitoring** NEW 2022	Premises monitored continuously for unauthorised physical access using CCTV, alarms, or guards
A.7.7	Clear desk and clear screen	Implement and enforce clear desk for paper/storage media and clear screen policy for IT equipment
A.7.10	Storage media	Manage lifecycle of storage media from acquisition through use to secure disposal/reuse
A.7.13	Equipment maintenance	Correctly maintain equipment to ensure availability and integrity; authorised maintenance only
A.7.14	Secure disposal or re-use of equipment	Verify that all sensitive data and licensed software is removed before equipment disposal or re-use

Annex A Controls — Theme 4: Technological

A.8 — 34 controls covering technical security measures (largest theme; includes 7 new/restructured controls)

Control	Title	Implementation note
A.8.1	User endpoint devices	Manage information stored on, processed on, or accessible via user endpoint devices
A.8.2	Privileged access rights	Allocate and use privileged access rights on a need-to-use basis; review regularly
A.8.3	Information access restriction	Restrict access to information and systems based on access control policy
A.8.4	Access to source code	Manage read and write access to source code, development tools, and software libraries
A.8.5	Secure authentication	Implement secure authentication technologies and procedures, including MFA where appropriate
A.8.6	Capacity management	Monitor and adjust resource utilisation to ensure required system performance
A.8.7	Protection against malware	Implement malware detection and prevention controls; user awareness
A.8.8	Management of technical vulnerabilities	Obtain information on technical vulnerabilities; assess exposure; take action; patch management
A.8.9	**Configuration management** NEW 2022	Define, document, implement, monitor, and review configurations including security configs for hardware, software, services
A.8.10	**Information deletion** NEW 2022	Delete information on systems, devices, and media when no longer required; verify deletion
A.8.11	**Data masking** NEW 2022	Mask PII and other sensitive data in non-production and third-party environments per policy
A.8.12	Data leakage prevention	Apply DLP measures to systems, networks, and devices processing sensitive information
A.8.13	Information backup	Maintain, test, and secure backup copies of information and software; test restorability
A.8.15	Logging	Produce, store, protect, and analyse event logs recording user activities, exceptions, faults
A.8.16	**Monitoring activities** NEW 2022	Monitor networks, systems, and applications for anomalous behaviour; set baselines; investigate alerts
A.8.20	Networks security	Protect networks and their supporting infrastructure; segregate, filter, and monitor
A.8.23	**Web filtering** NEW 2022	Filter access to external websites to reduce exposure to malicious content
A.8.24	Use of cryptography	Define and implement rules for effective use of cryptography including key management
A.8.25	Secure development life cycle	Establish and apply rules for secure development of software and systems
A.8.28	**Secure coding** NEW 2022	Apply secure coding principles to software development; training for developers; code review

Implementation tip: Theme 4 (Technological) is the most complex theme to implement. Prioritise controls A.8.8 (vulnerability management), A.8.15 (logging), and A.8.9 (configuration management) first — these three generate the most evidence for your Stage 2 audit and support multiple other controls.

Risk Assessment: Step-by-Step Worked Example

A practical walk-through of Clause 6.1.2 requirements using a sample organisation

Step 1 — Define Risk Criteria

Before assessing risks, document your likelihood and impact scales. Example 3-point scale:

Likelihood	Score	Meaning
Low	1	Unlikely to occur
Medium	2	Could occur occasionally
High	3	Expected to occur regularly

Impact	Score	Meaning
Low	1	Minor disruption
Medium	2	Significant disruption
High	3	Critical / regulatory breach

Step 2 — Risk Register Extract (Worked Example)

#	Asset	Threat	Vulnerability	L	I	Score	Rating
R01	Customer database	Unauthorised access	Weak password policy	3	3	9	HIGH
R02	Email system	Phishing attack	No MFA on remote access	3	2	6	HIGH
R03	Backup media	Physical theft	Tapes stored off-site unencrypted	2	3	6	HIGH
R04	HR records	Accidental disclosure	Shared folder with excess permissions	2	2	4	MEDIUM
R05	Office workstations	Malware infection	Patch cycle delayed >60 days	3	2	6	HIGH
R06	Cloud storage	Data leakage	No DLP controls in place	2	2	4	MEDIUM
R07	Visitor Wi-Fi	Network intrusion	Shared SSID with production	1	2	2	LOW

Risk acceptance threshold: In this example, scores of 6–9 = HIGH (require treatment), 3–5 = MEDIUM (monitor or treat), 1–2 = LOW (accept with documentation). Your organisation's risk appetite determines these thresholds — document them in your risk assessment methodology before scoring begins.

Risk Treatment Plan & Statement of Applicability

Clause 6.1.3 — How to build the SoA and link it to your risk register

Risk Treatment Options

Option	Meaning	When to use	Example
Treat / Mitigate	Implement controls to reduce risk	Risk score above acceptance threshold	Enable MFA on all remote access (R02)
Transfer	Move risk to third party (insurance, contract)	Risk is financial or operational	Cyber insurance for data breach costs
Avoid	Eliminate the activity that creates the risk	Risk is unacceptable and activity not essential	Stop storing unencrypted backup tapes off-site
Accept	Consciously accept the risk without action	Risk within appetite; cost of treatment exceeds impact	Accept R07 (visitor Wi-Fi low risk) with documented justification

Risk Treatment Plan Extract

Risk	Treatment	Control (Annex A)	Owner	Target Date	Status
R01	Mitigate	A.8.5 Secure authentication	IT Manager	30 Jun	In Progress
R02	Mitigate	A.8.5 MFA, A.6.7 Remote working	IT Manager	30 May	Complete
R03	Avoid + Treat	A.8.24 Cryptography, A.7.10 Media	Ops Manager	15 Jun	Planned
R04	Mitigate	A.8.3 Access restriction	HR Director	30 Jun	In Progress
R05	Mitigate	A.8.8 Vulnerability management	IT Manager	31 May	Complete

Statement of Applicability (SoA) — Sample Extract

The SoA must list all 93 Annex A controls. For each, state: Applicable (Yes/No), Justification, Implementation status, and link to risk(s) addressed.

Control	Title	Applicable	Justification	Status
A.5.1	Information security policies	✔ Yes	Required by Clause 5.2	Implemented
A.5.7	Threat intelligence	✔ Yes	R01, R02 — ongoing threat awareness	Partial
A.5.23	Cloud services security	✔ Yes	R06 — cloud storage in use	Planned
A.7.3	Securing offices	✘ N/A	Single site, existing physical controls sufficient; no sensitive processing areas	N/A
A.8.4	Access to source code	✘ N/A	Organisation does not develop software	N/A
A.8.11	Data masking	✔ Yes	R04 — PII in HR systems requires masking in test	Planned

Audit warning: Every "Not Applicable" entry in your SoA must carry a documented justification. An auditor will challenge any exclusion of controls from the four major groups — access control, cryptography, incident management, and business continuity — without robust evidence that they genuinely do not apply.

Mandatory Documentation Checklist

Every document ISO 27001:2022 requires — flagged by clause

Required Documents (must exist)

- ☐ **Clause 4.3:** ISMS Scope document
- ☐ **Clause 5.2:** Information Security Policy
- ☐ **Clause 6.1.2:** Risk assessment methodology
- ☐ **Clause 6.1.2:** Information security risk register
- ☐ **Clause 6.1.3:** Statement of Applicability (SoA)
- ☐ **Clause 6.1.3:** Risk Treatment Plan (RTP)
- ☐ **Clause 6.2:** Information security objectives
- ☐ **Clause 7.2:** Competence records / training records
- ☐ **Clause 8.1:** Operational planning criteria
- ☐ **Clause 8.2:** Risk assessment results
- ☐ **Clause 8.3:** Risk treatment results
- ☐ **Clause 9.1:** Evidence of monitoring & measurement
- ☐ **Clause 9.2:** Internal audit programme & results
- ☐ **Clause 9.3:** Management review records
- ☐ **Clause 10.1:** Nonconformity and corrective action log

Supporting / Best-Practice Documents

- ☐ Asset inventory / information asset register
- ☐ Access control policy and procedure
- ☐ Password / authentication policy
- ☐ Incident response plan and incident log
- ☐ Business continuity / DR plan
- ☐ Supplier security assessment records
- ☐ Awareness training programme and attendance log
- ☐ Cryptography policy (if encryption used)
- ☐ Data classification scheme and labelling guide
- ☐ Change management procedure
- ☐ Vulnerability management process
- ☐ Remote working / BYOD policy
- ☐ Clear desk and clear screen policy
- ☐ System hardening baselines / config standards
- ☐ Network architecture and security diagram

Document control tip: Every document must have a title, document ID, version number, date, owner, and review date. Stage 1 audit will verify that document control procedures (Clause 7.5) are applied consistently across all documented information — missing version control is a common minor NCR.

ISMS Implementation Roadmap

8-phase approach from project initiation to certification — typical timeline: 9–18 months

1

Phase 1 — Project Initiation (Weeks 1–3)

Secure top management commitment (documented). Appoint ISMS Manager and project team. Define high-level project scope. Budget resources. Establish steering committee with executive sponsor.

2

Phase 2 — Gap Analysis (Weeks 3–6)

Assess current state against ISO 27001:2022 clause and Annex A requirements. Document gaps. Prioritise remediation effort. Produce gap analysis report for management. Confirm final ISMS scope (Clause 4.3).

3

Phase 3 — Risk Assessment & Treatment (Weeks 6–14)

Document risk methodology. Build information asset register. Identify threats and vulnerabilities. Score all risks against criteria. Produce Risk Treatment Plan. Select Annex A controls. Produce first SoA draft.

4

Phase 4 — Documentation Build (Weeks 10–20)

Create all mandatory documented information (see Page 12). Develop policies, procedures, and work instructions. Establish document control system. Conduct management policy review and sign-off.

5

Phase 5 — Controls Implementation (Weeks 16–36)

Implement selected Annex A controls. Configure technical controls (logging, access control, vulnerability management, MFA). Train all staff on awareness programme. Begin collecting operational evidence.

6

Phase 6 — Internal Audit (Weeks 36–42)

Execute internal audit programme across all clauses and applicable controls. Raise NCRs. Root cause analyse all findings. Implement corrective actions. Verify corrective action effectiveness. Retain all evidence.

7

Phase 7 — Management Review (Week 44)

Conduct formal management review per Clause 9.3. Review audit results, KPIs, risk register, objective progress, incidents, and continual improvement opportunities. Document outputs and actions.

8

Phase 8 — Certification Audit (Weeks 46–52)

Stage 1 (documentation review) — certifying body reviews ISMS documentation; address any Stage 1 findings. Stage 2 (effectiveness audit) — on-site review of control implementation. Address any NCRs within agreed timeframe. Certificate issued.

Timeline note: 9–18 months is typical. Smaller organisations with mature security practices can achieve certification in 6–9 months. Complex multi-site enterprises may require 18–24 months. The largest time investment is Phase 5 (controls implementation) — plan accordingly.

Common Implementation Pitfalls

The top 10 mistakes organisations make — and how to avoid them

#	Pitfall	Why it fails	How to avoid it
1	Scope too narrow or too broad	Narrow scope misses critical assets; broad scope creates unmanageable audit burden	Define scope based on business risk, not what's convenient; document boundary justifications
2	Top management not engaged	ISMS becomes an IT project, not a business programme; policy never gets real authority	Require executive sponsor to chair management review; link ISMS to business objectives
3	Risk methodology applied inconsistently	Auditors spot inconsistencies in risk scores; SoA control selections can't be justified	Document methodology before scoring; use the same scales and criteria for every asset
4	SoA not kept current	Risk register changes but SoA not updated; control applicability decisions become stale	Link SoA version to risk register version; review SoA on every risk assessment cycle
5	Controls documented but not operating	Policy exists but no evidence of operation — auditors test effectiveness, not paperwork	Collect operational evidence continuously: logs, tickets, training records, access reviews
6	Internal auditors not independent	Teams audit their own areas; findings lack credibility; creates immediate NCR in Stage 2	Rotate auditors across teams; train auditors; use cross-functional pairs
7	Supplier controls ignored	A.5.19–A.5.22 frequently under-implemented; major finding in 60%+ of first-time audits	Add IS clauses to every supplier contract template; conduct annual supplier reviews
8	Awareness training not tracked	Clause 7.2/7.3 requires evidence of competence — no records means automatic NCR	Use LMS with completion tracking; assign mandatory annual refresher; retain records 3 years
9	Incident log empty or incomplete	Shows ISMS not operating; all organisations experience events — absence is a red flag	Lower reporting threshold; log near-misses; hold monthly incident review meetings
10	Not addressing 2022 new controls	Transitioning orgs often miss new controls — auditors specifically check A.5.7, 5.23, 8.9–8.11, 8.23, 8.28	Run a specific gap analysis against the 11 new controls before certification audit

Internal Audit Programme Design

Clause 9.2 — Building and executing a credible, independent internal audit programme

What the Standard Requires (Clause 9.2)

ISO 27001 requires the organisation to plan, establish, implement, and maintain an audit programme. Each audit must have a defined **scope, criteria, frequency** and must be conducted by **objective, impartial** auditors. Results must be reported to relevant management, and **documented information** retained as evidence.

Annual Internal Audit Programme Template

Audit Area	Clause / Controls	Frequency	Q1	Q2	Q3	Q4
Context & Scope	Clauses 4, 5	Annual	✔			
Risk Management	Clause 6.1–6.2	Annual		✔		
Operational Controls	Clauses 7, 8	Semi-annual	✔		✔	
Access Control	A.5.15–18, A.8.2–5	Semi-annual		✔		✔
Incident Management	A.5.24–5.28	Annual		✔		
Supplier Security	A.5.19–5.22	Annual			✔	
Technical Controls	A.8 (Theme 4)	Semi-annual		✔		✔
Physical Security	A.7 (Theme 3)	Annual			✔	
Improvement (NCR review)	Clause 10	Quarterly	✔	✔	✔	✔

NCR Classification Guide

Type	Definition	Example	Resolution time
Major NCR	Systematic failure of a requirement; no evidence a control exists	No risk assessment conducted; no SoA produced	Before Stage 2 / cert granted
Minor NCR	Isolated lapse in an otherwise functioning control	Two supplier contracts missing IS clause	Within 90 days of raising
Observation	Potential improvement area; not a non-conformity	Patch cycle meeting target but no trend analysis	Address at next review cycle

Auditor independence rule: ISO 19011 (the auditing guidelines standard) requires auditors to be objective and impartial. This means a member of the IT team cannot audit IT controls, and an HR manager cannot audit HR-related ISMS controls. Rotate auditors across functions and document independence in every audit report.

Management Review

Clause 9.3 — Inputs, outputs, and best practice for an effective management review

Clause 9.3 (2022 restructure): Management review is now divided into three sub-clauses: **9.3.1** (general — frequency and documentation), **9.3.2** (management review inputs — 9 required items), and **9.3.3** (management review results — what outputs must be documented). This is a testable change in certification exams.

Required Inputs (Clause 9.3.2)

1. Status of actions from previous management reviews
2. Changes in external and internal issues relevant to ISMS
3. Changes in needs and expectations of interested parties
4. Feedback on information security performance (including trends in NCRs, monitoring results, audit results)
5. Feedback from interested parties
6. Results of risk assessment and risk treatment plan status
7. Opportunities for continual improvement

Required Outputs (Clause 9.3.3)

- ☐ Decisions on continual improvement opportunities
- ☐ Any need for changes to the ISMS
- ☐ Resource needs identified and addressed
- ☐ Actions assigned with owners and due dates
- ☐ Updated information security objectives (where required)
- ☐ Minutes of management review meeting retained as documented information

Management Review — KPI Dashboard Template

KPI	Target	Q1 Actual	Q2 Actual	Trend
Security incidents reported	< 5/month	3	2	Improving
Critical vulnerabilities unpatched >30 days	0	4	1	Improving
Staff awareness training completion	> 95%	88%	96%	On target
Supplier assessments overdue	0	2	0	Cleared
Open NCRs from internal audit	< 3	7	3	Watch
Risk treatment plan actions complete	> 85%	70%	82%	Behind target
Access reviews completed on schedule	100%	100%	100%	On target

Preparing for Your Certification Audit

Stage 1 and Stage 2 readiness — what the certifying body will check

Stage 1 — Documentation Review ~1 Day

The certifying body auditor reviews your documented information to confirm the ISMS is defined and ready for Stage 2. They will check:

- ✔ ISMS scope document (Clause 4.3)
- ✔ Information security policy (Clause 5.2)
- ✔ Risk assessment results and methodology
- ✔ Statement of Applicability (all 93 controls addressed)
- ✔ Risk Treatment Plan with owner and dates
- ✔ Internal audit evidence (at least one cycle)
- ✔ Management review minutes
- ✔ Documented objectives and progress

Stage 2 — Effectiveness Audit 1–3 Days

Auditor visits (or remotely accesses) the organisation to verify controls are implemented and operating effectively. Key areas tested:

- ✔ Access control — live system walkthrough
- ✔ Incident log — reviewed for real entries
- ✔ Training records — spot-checked for individuals
- ✔ Vulnerability scan results — evidence of patching
- ✔ Supplier contracts — IS clauses verified
- ✔ Physical security — site walkthrough
- ✔ Corrective actions — evidence of closure
- ✔ Management review — interview with executives

30-Day Pre-Audit Readiness Checklist

- ☐ Complete final internal audit across all high-risk clauses and controls; close all major NCRs
- ☐ Verify SoA is up-to-date and signed by authorised management
- ☐ Run management review and produce signed minutes with all 9.3.2 inputs covered
- ☐ Check training records are complete and all staff have current year's awareness training
- ☐ Review access logs — ensure all leavers and movers have had access updated within 30 days
- ☐ Verify vulnerability scan has been run in the last 30 days with patching evidence for all criticals
- ☐ Confirm incident log has at least 6 months of entries (even near-misses count)
- ☐ Collect evidence pack: policies, logs, records, screenshots — one folder per Annex A control
- ☐ Brief all staff likely to be interviewed: know the policy, know their role, stay calm
- ☐ Prepare a walk-through guide for the auditor — maps to your scope and key areas

Certification success rate: Organisations that complete a full internal audit cycle with corrective actions closed before Stage 2 have significantly higher first-time pass rates. Don't skip the internal audit — it is the single best predictor of Stage 2 success.

GSDC Certification Pathway for ISO 27001

Programmes available for individuals who want to implement, audit, or lead ISO 27001

MOST POPULAR

ISO 27001 Lead Auditor

- → Conduct Stage 1 & Stage 2 certification audits
- → Lead audit teams for large programmes
- → Write NCRs and audit reports
- → Target: Consultants, CB auditors, senior CISO
- → Format: Online self-paced + live sessions
- → Exam: 58 questions, 70% pass mark

RECOMMENDED FOR IMPLEMENTERS

ISO 27001 Lead Implementer

- → Design and build an ISMS from scratch
- → Gap analysis and implementation management
- → Risk assessment and SoA development
- → Target: IS Managers, GRC teams, consultants
- → Format: Online self-paced + live sessions
- → Exam: Multiple-choice, 70% pass mark

FOR IN-HOUSE TEAMS

ISO 27001 Internal Auditor

- → Conduct internal ISMS audits
- → Report findings to management
- → Support Stage 2 preparation
- → Target: IT security teams, compliance officers
- → Format: Online self-paced
- → Exam: Online proctored assessment

TRANSITION TRACK

ISO 27001:2022 Conversion

- → For existing 2013 credential holders
- → Focused 2022 delta module
- → Covers 11 new controls in depth
- → Targeted conversion assessment
- → Fast-track to 2022 compliant credential
- → GSDC badge issued on passing

Why Choose GSDC?

150+	50K+	Online	SME
COUNTRIES WITH GSDC PROFESSIONALS	CERTIFIED GSDC PROFESSIONALS GLOBALLY	24/7 ACCESS, FLEXIBLE STUDY	CONNECT: LIVE EXPERT ACCESS

RELATED OFFER — ISO 27001 + ISO 27701 BUNDLE

Stack ISO 27001 & Privacy Certification for Maximum Impact

Combine ISO 27001 Lead Auditor with GSDC's ISO 27701 Privacy or ISO 22301 BCMS programme. Ask GSDC about bundle pricing and maximise your credential value.

EXPLORE GSDC BUNDLE OPTIONS →

Glossary of Key ISMS Terms

30+ essential definitions for ISO 27001:2022 implementers and auditors

Term	Definition
ISMS	Information Security Management System — the systematic framework of policies, processes, procedures, and controls for managing information security risks
SoA	Statement of Applicability — mandatory document listing all 93 Annex A controls with inclusion/exclusion decisions and justifications
CIA Triad	Confidentiality, Integrity, Availability — the three core objectives of information security
Risk appetite	The level and type of risk an organisation is willing to accept in pursuit of its objectives
Residual risk	The risk remaining after treatment controls have been applied; must be within risk appetite or accepted by management
Risk treatment	Process of selecting and implementing measures to modify risk — options include: mitigate, transfer, avoid, or accept
RTP	Risk Treatment Plan — document specifying how identified risks will be addressed, the controls selected, owners, timelines, and status
NCR	Non-Conformity Report — formal finding raised when evidence shows a requirement of the standard is not being met
PDCA	Plan-Do-Check-Act — the continual improvement cycle underlying all ISO management system standards
Interested parties	Persons or organisations that can affect, be affected by, or perceive themselves to be affected by the ISMS
Documented information	ISO term for any information an organisation needs to control and maintain — covers both documents (policies/ procedures) and records (evidence)
Control	Measure that modifies risk — can be a policy, procedure, practice, or technology; Annex A provides a catalogue of 93 reference controls
Stage 1 Audit	Documentation and readiness review — the first phase of the certification audit, conducted before Stage 2
Stage 2 Audit	Implementation effectiveness audit — the certifying body verifies the ISMS is implemented, operational, and achieving its objectives
Surveillance audit	Annual follow-up audit (in years 2 and 3 of the 3-year certificate cycle) to verify continued compliance and improvement
Recertification	Full audit conducted every 3 years to renew the ISO 27001 certificate
Threat intelligence	New in 2022 (A.5.7) — the collection, analysis, and application of information about threats to inform ISMS decisions
Data masking	New in 2022 (A.8.11) — concealment of sensitive data in non-production environments by replacing real values with realistic but fictional ones
Secure coding	New in 2022 (A.8.28) — application of security principles throughout the software development process to prevent vulnerabilities
ISO 27002	The companion standard to ISO 27001 — provides implementation guidance for Annex A controls but is not certifiable itself
ISO 19011	Guidelines for auditing management systems — the reference standard for internal auditor conduct, impartiality, and methodology
HLS / Annex SL	High-Level Structure — the common framework all ISO management system standards (27001, 22301, 9001, 14001) share, enabling easier integration
Vulnerability management	The cyclical practice of identifying, classifying, remediating, and mitigating security vulnerabilities in systems (A.8.8)
Corrective action	Action taken to address the root cause of a nonconformity so it does not recur — required by Clause 10.2

Final Action Checklist & Next Steps

Your implementation action plan — take one step at a time

Phase 1–4 Checklist (Foundation)

- ☐ Executive sponsor identified and committed
- ☐ ISMS Manager appointed with formal authority
- ☐ Gap analysis against ISO 27001:2022 complete
- ☐ ISMS scope documented and approved
- ☐ Risk assessment methodology documented
- ☐ Information asset register built and owned
- ☐ Risk register completed with scores
- ☐ Risk Treatment Plan with owners and dates
- ☐ Statement of Applicability (all 93 controls) produced
- ☐ Information security policy signed by CEO/MD
- ☐ All mandatory documents from Page 12 created
- ☐ Document control system in place

Phase 5–8 Checklist (Implementation)

- ☐ All selected Annex A controls implemented
- ☐ 11 new 2022 controls specifically addressed
- ☐ Staff awareness training complete with records
- ☐ Internal audit programme executed — full cycle
- ☐ All major NCRs from internal audit closed
- ☐ Management review conducted and minuted
- ☐ Certifying body selected and Stage 1 booked
- ☐ Stage 1 findings remediated before Stage 2
- ☐ Evidence pack prepared (one folder per control)
- ☐ 30-day pre-audit checklist (Page 17) complete
- ☐ Staff briefed for auditor interviews
- ☐ Certificate received — surveillance audit scheduled

Next Steps for Individuals

1. Identify which GSDC programme fits your role: Lead Auditor, Lead Implementer, Internal Auditor, or Conversion (see Page 18)
2. Visit gsdcouncil.org to review the full programme curriculum and enrolment options
3. Enrol and begin your certification journey — study at your own pace on GSDC Studio
4. Use SME Connect to get expert answers to implementation and exam questions
5. Pass your exam, receive your digital badge, and update your LinkedIn and CV

Ready to Implement ISO 27001:2022 and Get Certified?

GSDC's ISO 27001 certification programmes equip you with everything in this guide — and more — delivered by expert instructors with real-world implementation experience.

START AT GSDCOUNCIL.ORG →