Q.Factorial

ISO 27001

for Beginners

A plain-English guide to your
Information Security Management System

Q.Factorial
Where Quality meets
Science, Technology & Sustainability

What this guide covers

1. Why ISO 27001 exists — and what it asks of your business
2. Confidentiality, Integrity and Availability: the CIA triad
3. How the standard is structured (same framework as ISO 9001)
4. Information assets, threats and risks
5. The 93 controls — and why most breaches are human, not technical
6. How ISO 27001 connects to other standards
7. Jargon buster: the words auditors use, in plain English

© 2026 QFactorial Ltd

Why does ISO 27001 exist?

The problem it solves

Every organisation holds information that has value — customer data, financial records, intellectual property, operational systems. That information faces constant threats: from criminal attack, human error, insider risk and physical exposure.

ISO 27001 gives you a structured framework for protecting the Confidentiality, Integrity and Availability of your information — for the benefit of your organisation, your customers and the people whose data you hold.

What it gives you

- A systematic approach to identifying and treating information security risks
- Confidence for customers, partners and regulators that their data is protected
- Evidence of due diligence — increasingly required in procurement and contracts
- A framework that addresses people, processes and technology — not just IT
- The foundation for other security and data protection obligations

© QFactorial Ltd 2026

THE ISMS CONCEPT

ISMS — a part of your BMS

The Information Security Management System (ISMS) is not a separate IT system. It is **a part of your BMS** — the part that protects your information assets.

Same structure, same PDCA cycle as ISO 9001 — but focused on information security rather than quality.

ISMS

Information Security Management System

Manages your information assets, the threats they face and the controls that protect them. Same structure as your QMS — different focus.

BMS

Business Management System

Your integrated system — quality, information security and other disciplines managed together. One set of processes, one audit programme.

ISO 27001

The standard underneath

The internationally recognised standard that gives your ISMS credibility, consistency and certification readiness.

© QFactorial Ltd 2026

STRUCTURE — HOW IT'S ORGANISED

How ISO 27001 is organised

The same ten-clause structure as ISO 9001 — plus Annex A, a set of 93 controls unique to ISO 27001.



Annex A — 93 controls

Selected and justified in the Statement of Applicability (SoA) — unique to ISO 27001.

A5 Organisational
37 controls

A6 People
8 controls

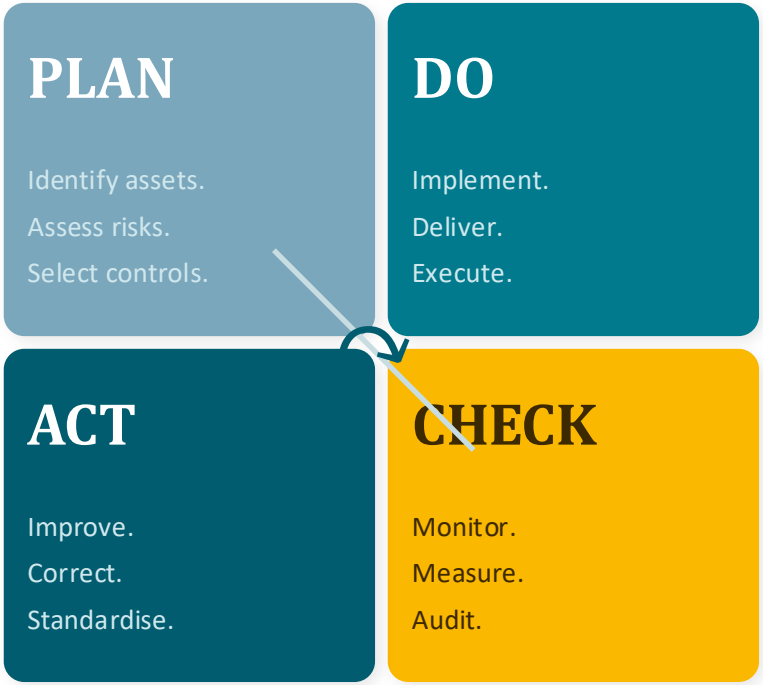
A7 Physical
14 controls

A8 Technological
34 controls

© QFactorial Ltd 2026

PDCA

Plan–Do–Check–Act applied to information security



How it maps to ISO 27001

PLAN *Clauses 4, 5, 6*

Understand your context, assess information security risks, select and plan controls

DO *Clauses 7, 8*

Put the resources in place and implement your controls

CHECK *Clause 9*

Monitor performance, conduct audits, review the system

ACT *Clause 10*

Fix what's not working, improve what is

© QFactorial Ltd 2026

KEY CONCEPTS

The concepts at the heart of ISO 27001

These ideas are fundamental to information security — and to understanding why the standard works the way it does.

C Confidentiality

Information is only accessible to those authorised to see it.

I Integrity

Information is accurate, complete and hasn't been tampered with.

A Availability

Information and systems are accessible when they are needed.

Information Assets

Anything of value to your organisation: data, systems, software, physical equipment, people's knowledge, processes. The ISMS exists to protect these.

Threats & Vulnerabilities

A threat is something that could harm an asset — a criminal, a careless employee, a power cut. A vulnerability is a weakness that a threat could exploit. Together they create risk.

Not just IT

Most information security incidents have a human cause — phishing, misdirected emails, lost devices, weak passwords, insider error. Technology controls alone are never enough.

© QFactorial Ltd 2026

CLAUSE 4 — CONTEXT

Understanding your information security context

What affects your ability to protect information — and who has a stake in how you do it.

4.1 嚼 Business context

What are the internal and external issues that affect your ability to achieve the intended outcomes of your ISMS?

4.2 吁 Interested parties

Who has a stake in your information security? Customers, regulators, partners, staff — and what do they require of you?

4.3 圈 Scope of your ISMS

Which information assets, systems and processes are covered? Scope must be documented and justified.

4.4 允 The ISMS itself

Establish, implement, maintain and continually improve an ISMS — including the processes needed and how they interact.

© QFactorial Ltd 2026

CLAUSE 5 — LEADERSHIP & COMMITMENT

Leadership & commitment

ISO 27001 requires top management to take personal accountability for the ISMS — not just to authorise it.

Leadership commitment

5.1

Top management establishes the information security policy, provides resources, supports the ISMS and promotes continual improvement.

Information Security Policy

5.2

A documented commitment to protecting information assets and meeting relevant obligations. Signed by top management and communicated across the organisation.

Roles & responsibilities

5.3

Clear ownership of the ISMS and its processes. Roles communicated within the organisation — a 2022 requirement.

Stakeholder focus

5.1

Top management ensures the organisation understands the requirements of relevant interested parties — customers, regulators, partners — and addresses them through the ISMS.

© QFactorial Ltd 2026

Planning: for security and performance

6.3

New in ISO 27001:2022 — Planning of changes: changes to the ISMS must be planned and managed to protect its intended outcomes.

6.1

Risk Assessment

Identify information assets and the threats and vulnerabilities they face. Evaluate the risk — considering CIA impact and likelihood. Document the process and results.

6.1

Risk Treatment

Decide how to respond to each risk: treat (apply controls), tolerate, terminate or transfer. Select controls from Annex A or elsewhere. Document your choices.

6.1

Statement of Applicability

The SoA lists all Annex A controls, states whether each is applied, and justifies inclusions and exclusions. Unique to ISO 27001 — a key audit document.

6.2

Information Security Objectives

Measurable targets for security performance. Connected to policy, risk treatment and monitored over time.

© QFactorial Ltd 2026

CLAUSE 7 — SUPPORT

Support: the resources behind your ISMS

Clause 7 is nearly identical to ISO 9001 — but awareness and competence carry extra weight in information security.

7.1 Resources

People, infrastructure, environment. Are you adequately resourced to protect your information assets?

7.2 Competence

People who affect information security must be competent. Security awareness and training are the primary defence against human-channel breaches.

7.3 Awareness

Everyone must understand the information security policy, their contribution to the ISMS and the consequences of not complying.

7.4 Communication

Internal and external communication on information security matters. Who needs to know what, when, and how?

7.5 Documented information

The documents and records that prove your system works. Controlled, accessible, up to date.

© QFactorial Ltd 2026

CLAUSE 8 — OPERATION

Operation: implementing your controls

Clause 8 is where the planning becomes reality — executing and maintaining the risk treatment plan.

8.1 Operational planning & control

Plan, implement, control, monitor and review the processes needed to meet information security requirements.

Manage planned changes and review unintended ones. Control outsourced processes that affect information security — external providers are a significant source of risk.

People controls, physical controls and technology controls must all be operating as planned. The ISMS doesn't protect anything if the controls exist only on paper.

8.2 Information security risk assessment & treatment

Risk assessments must be performed at planned intervals and when significant changes occur.

Risk treatment plans must be implemented and their effectiveness confirmed.

Both must be documented — the risk register and treatment plan are core ISMS records.

© QFactorial Ltd 2026

Annex A: 93 controls across four themes

Not all controls apply to every organisation. The Statement of Applicability (SoA) records which are included, which are excluded, and why.

A5 Organisational

37 controls

Policies, roles, responsibilities, asset management, supplier relationships, incident management, business continuity and legal compliance. The broadest theme — sets the framework within which everything else operates.

A6 People

8 controls

Screening, terms of employment, awareness, training, disciplinary processes, remote working and confidentiality agreements. This is where the human factor is explicitly addressed — often the weakest link and the most overlooked.

A7 Physical

14 controls

Secure areas, equipment protection, clear desk, physical media disposal, physical security monitoring. Physical access to information and systems is as much a risk as digital access.

A8 Technological

34 controls

Access control, cryptography, malware protection, logging, monitoring, vulnerability management, secure configuration, data leakage prevention and secure coding. Technology controls are necessary but not sufficient.

© QFactorial Ltd 2026

OUTSOURCING & CLOUD

What if my IT or data processing is outsourced?

Outsourcing your IT or data processing doesn't outsource the risk — or your accountability.

You remain accountable

If a supplier suffers a breach that exposes your data, your organisation is still responsible for protecting that information. Your ISMS scope must cover all information assets — including those held or processed by third parties on your behalf.

Suppliers must be managed

ISO 27001 Annex A controls A5.19–A5.22 cover supplier relationships specifically. You need documented security requirements in contracts, evidence of supplier controls, and a process for monitoring and reviewing supplier security performance.

Cloud has its own control

A5.23 (new in 2022) requires specific processes for cloud services — covering security requirements when adopting, managing and exiting cloud services. If you use cloud-hosted systems, this control almost certainly applies.

The right questions to ask

Does your IT provider have ISO 27001 certification — or equivalent evidence of security controls? What happens to your data if the contract ends? Who can access your data, and under what circumstances? These are ISMS questions, not just commercial ones.

© QFactorial Ltd 2026

Performance evaluation: is your ISMS working?

9.1

Monitoring & measurement

Monitor the ISMS, its controls and information security performance. Use data to understand what's happening — not just gut feel.

9.2

Internal audits

Regular structured checks of the ISMS against the standard and your own requirements. Evidence that controls are operating, not just documented.

9.3

Management review

Top management reviews ISMS performance at planned intervals. Inputs include risk status, objective achievement, audit findings and changes to context.

© QFactorial Ltd 2026

CLAUSE 10 — IMPROVEMENT

Improvement: the point of it all

ISO 27001 doesn't require zero security incidents. It requires a system that learns from them and gets stronger.

10.1 — Continual improvement

This isn't about fixing problems. It's about making the ISMS stronger even when things are working.

Sources of improvement ideas:

- Audit findings and observations
- Security incidents and near misses
- Threat intelligence and emerging risks
- Changes to the information security landscape
- Management review outputs

10.2 — Nonconformity & corrective action

When something doesn't meet a requirement — or when a security incident occurs — ISO 27001 requires you to act at three levels.

First, deal with the immediate problem and contain any damage. Second, investigate the root cause so it doesn't recur. Third, check that the action worked.

All nonconformities and corrective actions must be documented.

© QFactorial Ltd 2026

DOCUMENTS & RECORDS

Documented information — what you need to keep

ISO 27001 is less prescriptive than most people expect. Each organisation decides what to document based on risk, complexity and the nature of its information assets.

Documents

How you intend to protect your information

ISO 27001 requires specific documents including an Information Security Policy, the scope of the ISMS, and the Statement of Applicability. The risk assessment methodology, risk register and risk treatment plan are also required documented information.

Some Annex A controls also call for topic-specific policies. One policy can cover more than one control, and the right number for your organisation is far fewer than 93 — more on this overleaf.

Records

Evidence that you worked as planned

Records prove the ISMS is operating as intended. ISO 27001 requires records of competence, monitoring and measurement results, internal audit findings, management review outputs and the results of corrective actions.

Records of control operation — evidence that your security controls are actually being followed — are equally important.

© QFactorial Ltd 2026

POLICIES — THE RIGHT NUMBER

93 controls. Not 93 policies.

One of the most common and costly mistakes in ISO 27001 implementation — and one of the easiest to avoid with the right guidance.

What the standard actually requires

ISO 27001 mandates a small set of core documents. Some Annex A controls reference topic-specific policies — on areas such as access control or supplier security. But a well-designed ISMS resolves these efficiently: one document can address multiple controls, and controls take many forms beyond written policy.

What often happens in practice

Template-driven implementations generate policies for every conceivable topic regardless of organisational need. They accumulate, fall out of date, and become a maintenance burden. Auditors who accept policy existence as evidence of compliance are not auditing the system — they are auditing the filing cabinet.

The right approach

The right number of policies depends on the organisation — its size, complexity, risk profile and how its controls are implemented. A well-designed ISMS means each document has a clear purpose, proportionate to actual risk and complexity. Fewer documents, lower ongoing cost, and a system that genuinely improves security.

The same mistake is already being made with AI

Just like templates, AI tools can generate comprehensive, audit-ready-looking ISMS documentation rapidly. The result is usually maximum paperwork dressed as a bespoke system. The trick is in knowing what to ask for — and what to leave out.

© QFactorial Ltd 2026

YOUR ISMS

How your ISMS works in practice

ISMS/BMS Description

Typically an ISMS or overarching BMS Manual, but not necessarily. Includes topic-specific policies where required.

Information Security Policy

Leadership's commitment to CIA. Signed. Communicated to everyone.

Risk Register & SoA

Your assets, threats, risks and control choices. The foundation of the ISMS.

Live Trackers

Examples: objectives tracker, action tracking, audit programme, KPI dashboard, document register.

Records & Evidence

Proof that the system is working and information is being protected.

© QFactorial Ltd 2026

INTEGRATION

ISO 27001 in your broader compliance framework

ISO 27001 uses the same High Level Structure as ISO 9001 — they integrate naturally within a single BMS.

Your information security & governance strategy

Sector, regulatory and contractual obligations specific to your organisation

ISO 27001 — and the ISO 27000 family

ISO 27004 (metrics), ISO 27005 (risk), ISO 27017/18 (cloud & PII), ISO 27701 (privacy) for depth and nuance

Standards that integrate naturally with ISO 27001

ISO 9001, ISO 14001, ISO 22301, ISO 42001 (all HLS-based)

Your BMS — quality, ESG, H&S, security and sustainability

One framework, one set of processes, one management review

A well-designed management system is the foundation that makes broader security and sustainability commitments credible and auditable.

© QFactorial Ltd 2026

ISO 27001 & GDPR

We did some GDPR work — where does that fit?

ISO 27001 and UK GDPR are complementary — not interchangeable. Understanding the relationship matters.

What UK GDPR requires

UK GDPR requires organisations to implement appropriate technical and organisational measures to protect personal data, but it does not prescribe exactly what those measures should be.

It also requires you to demonstrate accountability: that you have assessed the risks to personal data and taken proportionate steps to address them.

Data breach notification, data subject rights, retention policies and privacy by design all require documented, repeatable processes.

What ISO 27001 provides

ISO 27001 certification provides substantial evidence of the technical and organisational measures required under UK GDPR, particularly Articles 25 (data protection by design) and 32 (security of processing).

The risk assessment methodology maps well to Data Protection Impact Assessment (DPIA) thinking. Annex A controls directly address many GDPR obligations: access control, encryption, breach response and retention.

For organisations needing a formal bridge, ISO 27701 extends ISO 27001 specifically to cover personal data — creating a Privacy Information Management System (PIMS) — recognised as strong evidence of GDPR compliance and part of the ISO 27000 standard family.

© QFactorial Ltd 2026

AUDIT PREPARATION

What the auditor looks for

ISO 27001 auditors follow the same verification logic as any ISO auditor — but with a specific focus on risk, controls and the human layer.

Is the risk assessment documented, repeatable and linked to the Statement of Applicability?

Are the selected controls from Annex A actually operating — not just documented?

Is there evidence that people understand their information security responsibilities?

Are security incidents and near misses being recorded, investigated and learned from?

Is top management actively and visibly involved in the ISMS — not just at arm's length?

© QFactorial Ltd 2026

YOUR ROLE

Your role as ISMS Coordinator

You don't own information security. You own the system that manages it.

圈 Keep the ISMS current

Risk register, SoA, policies and records — all maintained. When the business changes, the ISMS follows.

傯 Feed the Live Trackers

Security objectives, KPIs, action tracking, audit programme. Regular updates — not annual scrambles.

煒 Run internal audits

Plan, conduct and report internal audits to the programme. Log findings. Track actions to closure.

杷 Support management review

Compile the input pack, attend the review, chase the action list.

屆 Be the bridge

Between leadership (who own information security policy) and the team (who generate the risk). Not the security police — the security partner.

滷 Live the role

Be the champion and gatekeeper of the ISMS. Set the example, keep the standard, and advocate for a security-aware culture.

© QFactorial Ltd 2026

JARGON BUSTER

Jargon buster

Information security terms — in plain English.

Common ISO management system terms are covered in our Beginners Guide to ISO 9001.

CIA triad

Confidentiality, Integrity and Availability — the three goals that every information security control ultimately serves.

Information asset

Anything of value that holds, processes or transmits information: data, systems, software, people's knowledge, physical devices.

Threat

Something that could cause harm to an information asset — a criminal, a careless employee, a natural disaster, a software vulnerability.

Vulnerability

A weakness that a threat could exploit. Unpatched software, weak passwords, unlocked doors and untrained staff are all vulnerabilities.

Risk

The combination of a threat, a vulnerability and the potential impact. Risk drives control selection.

Control

A measure taken to reduce risk — a policy, a technical safeguard, a training programme, a physical lock.

Statement of Applicability (SoA)

The document that lists all 93 Annex A controls, states which apply and why, and justifies any exclusions. Unique to ISO 27001.

Risk treatment

The decision about how to respond to a risk: treat it (apply controls), tolerate it, terminate the activity, or transfer it (e.g. insurance).

ISMS

Information Security Management System. The part of your BMS that manages information security risks and controls.

Incident

Any event that compromises or threatens the Confidentiality, Integrity or Availability of information — from a data breach to a misdirected email.

© QFactorial Ltd 2026

Q.Factorial

Where to start

1. Map your information assets — what do you hold, where does it live, who can access it?
2. Identify the threats and assess the risks — what could go wrong and how seriously?
3. Select and implement controls — starting with the highest risks and the human layer
4. Build the ISMS into your existing management system — don't create a separate one

Keep in mind

- Confidentiality, Integrity, Availability — every control serves one of these.
- Most breaches are human. Train, remind and build a security culture.
- Know your assets. Know your risks. Keep both current.
- Your ISMS is a part of your management system — not a separate burden.
- The aim: reduce information security risk and improve year on year.

© 2026 QFactorial Ltd