

A short primer on ISO/IEC 27001

What the standard is, why it's built on risk, and how it connects to our workshop.

READING TIME ~8 minutes · NO PRIOR KNOWLEDGE NEEDED · SKIM THE TABLES IF SHORT ON TIME

You don't need to memorise a standard to take part in the workshop. The goal of this primer is simply to give you the *language* of information-security risk, so that when we talk about assets, controls, likelihood and impact, it all fits into a bigger, real-world picture. That picture is ISO/IEC 27001.

What ISO/IEC 27001 actually is

ISO/IEC 27001 is the leading international standard for an **Information Security Management System (ISMS)** — the set of policies, processes, people and decisions an organisation uses to keep its information secure.^[1] The current edition is **ISO/IEC 27001:2022**. Two things are worth underlining:

- It is a **management system**, not a product or a piece of software. You can't buy your way to it; you build and run it.
- An organisation can be independently **audited and certified** against it — which is why customers, investors and regulators often ask for it.

Everything in the standard serves one aim: protecting information across three dimensions, the classic **CIA triad** — **Confidentiality** (only the right people see it), **Integrity** (it isn't wrongly changed) and **Availability** (it's there when needed).

The core idea: it's built on risk

This is the part that matters most for our workshop. ISO/IEC 27001 does not hand you a fixed checklist of things to do. Instead, it requires you to **assess and treat information-security risks** and to choose your protections based on what those risks actually are.^[1] In the standard, the requirement to run an information-security *risk assessment* and *risk treatment* sits at its heart (Clause 6.1). In other words: **risk assessment is the engine of the whole standard** — the same engine you'll be running by hand in the workshop.

WHY THIS DESIGN

Two organisations can both be "ISO 27001 compliant" and protect very different things — because each one's controls follow its own risks. A hospital and a game studio don't face the same threats,

Annex A: the catalogue of controls

Once you know your risks, you need *controls* to treat them. ISO/IEC 27001:2022 ships with **Annex A**, a reference catalogue of **93 controls** grouped into four themes.^{[1][6]} The 2022 edition reorganised the older set of 114 controls (across 14 domains) into this simpler structure:

37 ORGANIZATIONAL	8 PEOPLE	14 PHYSICAL	34 TECHNOLOGICAL
----------------------	-------------	----------------	---------------------

Crucially, **Annex A is not a mandatory to-do list**. It's a menu. You select the controls that address *your* assessed risks and record your choices — and your reasons for leaving others out — in a document called the **Statement of Applicability (SoA)**.^[7] Risk assessment comes first; controls follow.

The family of standards around it

ISO/IEC 27001 doesn't stand alone. A few relatives are worth recognising by name:

Standard	What it gives you
ISO/IEC 27002	Practical implementation guidance for each Annex A control. ^[2]
ISO/IEC 27005	Guidance specifically on managing information-security risk — the method our workshop borrows (identify → analyse → evaluate → treat). ^[3]
ISO 31000	General risk-management principles that apply to any risk, not just security. ^[4]
NIST SP 800-30	A widely used US guide for conducting risk assessments; same core idea of threat × vulnerability × impact. ^[5]

How this connects to our workshop

The exercise you'll run in your group is a hands-on, small-scale version of the exact risk cycle an ISMS runs continuously. Here's the direct mapping:

In the workshop you will...	...which mirrors this in ISO 27001 / 27005
List your systems (the Assets tab)	Establishing scope & identifying assets — the boundary of what you're protecting
Identify what could go wrong	Risk identification (Clause 6.1.2 / ISO 27005)
Score Likelihood × Impact	Risk analysis & risk evaluation — deciding which risks matter most

Choose a response — the 4 T's	Risk treatment options (Clause 6.1.3): Treat =modify/reduce · Tolerate =retain/accept · Transfer =share · Terminate =avoid
Keep a risk register	The documented results of the risk assessment — an ISMS keeps this as a living record
Re-score the residual risk & track status	Monitoring and continual improvement (the Plan–Do–Check–Act loop)

The one thing to take away

A real ISMS is, at its core, this loop run forever: know your assets, find the risks, weigh them, treat them, watch them. In the workshop you'll do one lap of that loop yourselves — which is the best possible way to understand what a standard like ISO 27001 is really asking organisations to do.

References & further reading

1. ISO/IEC 27001:2022 — *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization. [iso.org/standard/27001](https://www.iso.org/standard/27001)
2. ISO/IEC 27002:2022 — *Information security controls*. ISO. [iso.org/standard/75652.html](https://www.iso.org/standard/75652.html)
3. ISO/IEC 27005:2022 — *Guidance on managing information security risks*. ISO. [iso.org/standard/80585.html](https://www.iso.org/standard/80585.html)
4. ISO 31000:2018 — *Risk management — Guidelines*. ISO. [iso.org/iso-31000-risk-management.html](https://www.iso.org/iso-31000-risk-management.html)
5. NIST SP 800-30 Rev. 1 — *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology. csrc.nist.gov/pubs/sp/800/30/r1/final
6. ISMS.online — *ISO 27001:2022 Annex A Controls explained*. isms.online/iso-27001/annex-a-2022/
7. PECB — *Understanding ISO/IEC 27001:2022 Annex A Controls & the Statement of Applicability*. pecb.com/en/article/understanding-isoiec-270012022-annex-a-controls

Standards summaries are paraphrased for teaching; consult the official ISO/IEC texts for authoritative wording. NIST publications are US Government works in the public domain.