

What is an asset?

A field guide to spotting the things worth protecting — before the workshop begins.

READING TIME ~7 minutes · PAIRS WITH THE ASSETS TAB IN THE WORKBOOK

In the workshop, the very first thing your group does is list your *assets*. It sounds simple, but it's the step that makes everything after it possible: **you can't assess a risk to something you haven't named**. Assets draw the boundary around what you're protecting. This guide explains what an asset is, the two kinds that matter, and exactly what to write down.

A working definition

Across the major standards, the idea is the same: an asset is **anything that has value to the organisation and therefore needs protecting**. NIST puts it plainly — an asset is “anything that has value to a person or organization”^[3] — and elsewhere describes assets as the data, people, devices, systems and facilities that let an organisation do its work.^[4]

KEY POINT

Value can be **tangible** (a server, a laptop) or **intangible** (customer data, source code, a reputation, know-how).^[3] Intangible assets are often the most valuable — and the easiest to overlook.

Two kinds of asset (and why the difference matters)

ISO/IEC 27005 — the risk-management guidance behind ISO 27001 — splits assets into two useful groups:^[1]

Primary assets

Information and business processes. The things that carry real value: customer/patient data, source code, financial records, the process of shipping a release or onboarding a user. This is what you actually care about.

Supporting assets

What the primary assets rely on: hardware, software, networks, people, sites and organisational structures — servers, laptops, databases, SaaS tools, the team itself.

THE INSIGHT

A supporting asset is usually **replaceable**; the information it holds often is **not**.^[1] A laptop can be swapped in a day — the only copy of a customer database cannot. That's why risk work protects the *information* first.

The lens that turns an asset into risks: C-I-A

For every asset, ask three questions. Each one exposes a different family of risk and feeds straight into the register:

- **Confidentiality** — what happens if the wrong people see it? (leak, breach, exposure)
- **Integrity** — what happens if it's wrongly changed or corrupted? (tampering, bad data, faulty deploy)
- **Availability** — what happens if it's gone when you need it? (outage, data loss, ransomware)

What counts as an asset in *this* workshop

We're looking at software and the systems around it, so keep it concrete. Use these categories as a checklist to jog your thinking:

Information & data — customer/patient records, PII, source code, secrets & credentials, configuration, databases, backups, logs

Software & services — your application, APIs and microservices, the CI/CD pipeline, admin tools, key third-party SaaS

Infrastructure & platform — cloud accounts, servers & containers, networks, developer laptops and endpoints

People & knowledge — key engineers, on-call cover, documentation, the "only-one-person-knows-this" knowledge

Processes — deployment, access management, incident response, onboarding/offboarding

Third-party & supply chain — vendors, open-source dependencies and libraries (SOUP), external APIs you depend on

Getting the altitude right

The commonest mistake is choosing the wrong level of detail. Aim for the level you can actually own and reason about.

- **Too granular** — listing every file or table. You'll drown before you assess anything.
- **Too broad** — "the whole platform" as one asset. Too vague to find real risks.
- **Just right** — "Patient database", "CI/CD pipeline", "customer-facing API". Nameable, ownable, and something you can picture failing.

For each asset you keep, do three quick things: give it an **owner**, flag whether it holds **personal data** (this is what brings GDPR into scope), and rate its **criticality**. These are exactly the columns waiting for you on the Assets tab.

Column on the Assets tab	What to write — <i>example</i>
System / application	Patient database (Postgres)
Owner	Platform team
Lifecycle status	In use
Type of information	Health data / PII
Personal data	Yes
Criticality	High

A 5-minute head start before you arrive

Jot down the 8–10 systems and data stores your team touches most. Mark which ones hold personal data. Circle the 3 you'd least like to lose or leak. Those three are where your group's risk work will begin — and you'll already be ahead.

References & further reading

1. ISO/IEC 27005:2022 — *Guidance on managing information security risks* (primary vs. supporting assets). ISO. [iso.org/standard/80585.html](https://www.iso.org/standard/80585.html)
2. ISO/IEC 27000:2018 — *Information security management systems — Overview and vocabulary* (definition of "asset"). ISO. [iso.org/standard/73906.html](https://www.iso.org/standard/73906.html)
3. NIST SP 800-160 Vol. 1 Rev. 1 — *Engineering Trustworthy Secure Systems* ("anything that has value..."). NIST. csrc.nist.gov/pubs/sp/800/160/v1/r1/final
4. NIST IR 8286 — *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. NIST. csrc.nist.gov/pubs/ir/8286/final
5. NIST SP 800-30 Rev. 1 — *Guide for Conducting Risk Assessments* (assets, threats, vulnerabilities). NIST. csrc.nist.gov/pubs/sp/800/30/r1/final
6. NIST Computer Security Resource Center — *Glossary: "asset"*. csrc.nist.gov/glossary/term/asset

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.