Know What You Have:

The First Step in Managing Cyber Risk

> **Good cyber risk decisions start with knowing what you have and what matters most.**

Senior leaders often get pulled into cyber conversations at the worst possible time: after an incident, during an audit, or when a supplier change goes wrong. In those moments, the questions are predictable:

- What systems and services are truly critical?
- Where is the sensitive data?
- Who owns each element, and who's accountable for fixing issues?
- What would break if we had to isolate a supplier, a device group, or a cloud service?

If the organisation can't answer those questions quickly and consistently, it's usually because there's no reliable, up-to-date view of what exists and how it connects.

Before risks can be mapped to controls (and controls to evidence), you need a dependable view of the systems, data, and suppliers those controls are meant to protect.

"Assets" in the real world

Most people hear "asset management" and think "laptops and servers." That's part of it, but a leadership-level view needs to cover the things the organisation relies on to deliver services and manage risk.

A practical view of assets includes:

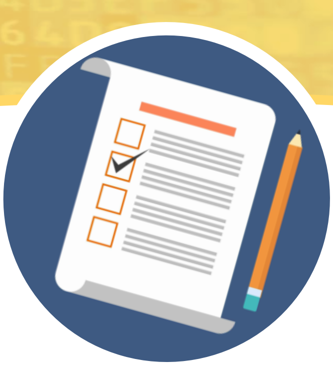
- **Devices:** laptops, mobiles, servers, network equipment, operational/IoT devices
- **Software & cloud services:** business applications, SaaS platforms, cloud subscriptions, automation tooling
- **Data:** key datasets (e.g., customer, financial, operational), important reports/exports, and where that data lives
- **Suppliers and outsourced services:** the services third parties provide and what those services support or connect to

And to manage those assets properly, you also need visibility of the relationships around them, such as:

- **Ownership:** who is accountable for each critical asset/service
- **Identity & access paths:** how people, service accounts, privileged access, and third parties reach or administer those assets

Know What You Have:

The First Step in Managing Cyber Risk



> *The aim isn't to create admin. It's to create clarity, so cyber risk decisions are based on what's actually in use, who owns it, and what matters most.*

Why asset visibility breaks (and what it looks like when it does)

In audits and assurance reviews, "asset management" is often technically present but practically weak. Common issues include:

- **Multiple lists, no single truth**:
  Procurement has one view, IT has another, security has another, and none match.
- **Ownership is unclear**:
  "IT" is listed as owner for everything, which really means nobody is accountable.
- **Inventories aren't decision-ready**:
  You can list items, but you can't prioritise them by business impact.
- **Shadow tooling becomes normal**:
  A team adopts a SaaS tool for speed, and it quietly becomes critical.
- **Supplier services are invisible**:
  You can name the supplier, but not the services, integrations, or data pathways.

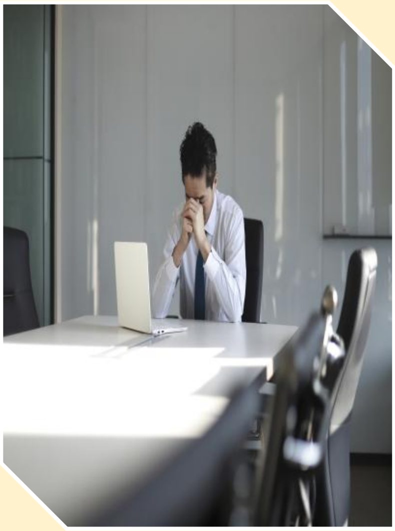
When these exist, leaders end up funding controls that *sound* sensible, but don't reliably cover what the organisation actually runs.

Examples leaders instantly recognise

These are the "small" issues that become big risks:

- **A laptop is lost:** but nobody can confirm whether it was encrypted, who it was assigned to, or whether it can be remotely wiped.
- **A leaver exits:** but access to two SaaS platforms persists because the accounts weren't tied back to a known service owner.
- **A team renews a tool:** but the organisation can't explain what data it holds, where it's hosted, or who approved it.
- **A supplier has an incident:** but the business can't quickly identify which services rely on them and what contingency exists.
- **A "temporary" cloud environment becomes production:** with no formal owner, no lifecycle plan, and no monitoring coverage.

These aren't edge cases. They're exactly what leaders get asked about when something goes wrong.



The maturity ladder: from “we have a list” to “we can run the business”

You don’t need to move immediately to an enterprise platform. What matters most is trustworthiness (is it accurate?) and freshness (does it stay current?).

Level 1 BASIC

A spreadsheet (or simple register)

With a nominated owner and a regular cadence of review.

What it’s good for:

- Quick visibility of critical devices/services
- Starting point for ownership and prioritisation

Where it breaks:

- It drifts unless updates are built into normal processes

Level 2 MANAGED

A central register

Owned by IT/ops (often inside an IT service tool), used for day-to-day operations.

What changes here:

- Assets are recorded as part of onboarding/procurement
- Changes are more likely to be reflected

Level 3 JOINED-UP

Discovery and operational processes feed the register.

Typical ingredients:

- Auto-discovery from endpoint/device management
- Integrations with cloud directories and identity lifecycle (joiners/movers/leavers)
- Supplier onboarding/offboarding captured as a standard workflow
- Exceptions reviewed (because discovery will always find surprises)

Level 4 RELIABLE

The inventory becomes a decision system

You can:

- Prioritise protection by criticality and business impact
- Rapidly scope incidents (“what is affected?”)
- Prove coverage (“what is monitored / managed / supported?”)
- Demonstrate lifecycle control (including end-of-life and supplier exit)

This is the level where senior leadership stops hearing opinions and starts receiving confident answers.

A simple model for ownership (that actually works)

Ownership is where asset management becomes risk management.
A practical split:

- **Business owner**: accountable for the service's value, impact, and risk acceptance
- **Service/technical owner**: accountable for operational delivery (change, patching, configuration, resilience)
- **Data owner (where relevant)**: accountable for data use, access model, and retention

If ownership is "everyone", accountability becomes "no one".
Standards such as the CIS Controls reinforce that unmanaged/unauthorised assets increase exposure and should be identified and addressed.

How to keep it current without creating admin overhead

The single best principle: inventories stay accurate when updates are triggered by business-as-usual events.

Examples of events that should update the inventory:

- Procurement and renewals
- Onboarding new systems and suppliers
- Change approvals and releases
- Identity lifecycle changes (joiners/movers/leavers)
- New cloud subscriptions/projects being created
- Devices being issued, repaired, returned, or retired

The UK NCSC describes asset management as the creation and maintenance of an asset inventory to ensure assets are accounted for, and emphasises the importance of understanding what assets an organisation has.

Know What You Have:
The First Step in Managing Cyber Risk

Self-check for senior leaders

If you asked for this today, could your organisation provide it confidently?

1. A list of your top critical services/systems
2. The named owner for each one
3. Where each service is hosted / who runs it
4. The key suppliers involved and what they provide
5. The most important data each service handles and where it lives
6. Confirmation that access is controlled (including leavers)
7. A view of what's end-of-life or running without support

If the answer is "we could pull that together over a few weeks," you've found a high-leverage cyber risk gap.

Where Tickbox can help

Tickbox provides assurance and advisory support to help organisations gain confidence and clarity over their asset management, strengthening how asset ownership, criticality, and supplier dependencies support cyber risk management and decision-making when it matters.

If you want to strengthen your cyber risk management, start by getting clear visibility, and drop us a message or email rebecca.dyson@tickboxsolutions.co.uk.