Asset Management in Information Security

THE ULTIMATE GUIDE

KORDON

Table of Contents

What Is This Book About?

As an information security manager, you already understand the importance of asset inventory management. You know that having a clear and accurate picture of your organisation's assets - whether physical, digital, or human - is essential for building a strong security posture. Asset inventory management isn't just about compliance; it's about ensuring that every critical asset is accounted for, protected, and integrated into your broader Information Security Management System (ISMS).

The real challenge, however, lies in doing this efficiently with limited resources. Security teams are often stretched thin, and keeping your asset inventory up-to-date while integrating it across your ISMS can feel like a daunting task. There's always room for improvement, and many security frameworks like ISO 27001, DORA and NIS2 expect to see such improvement and evolution within your Information Security Management System (ISMS) over time.

This resource is designed for security managers who are already familiar with the fundamentals but want to optimise, streamline, and scale their asset management processes. Inside, you'll find actionable tips that help you make the most of your resources while meeting the growing demands of security and compliance.

I'll focus on practical steps you can take to move beyond basic inventory tracking, using modern tools, processes, and collaboration to turn asset management into a strategic asset that continuously supports security, compliance, and operational resilience.

What is Asset Inventory Management?

Before diving into the specifics of how to take your asset management process to the next level, it's important to establish a clear understanding of what asset management means within the context of an Information Security Management System (ISMS) and why it plays such a vital role in supporting your overall security strategy.

Asset management in an ISMS is the process of identifying, tracking, classifying, and securing all of the assets - both digital and physical - that are critical to your organisation's operations. Assets can include everything from hardware (servers, laptops, mobile devices) and software (applications, licences) to intellectual property, physical property, data, and even personnel who have privileged access to sensitive systems.

The goal of asset management is not only to maintain an accurate inventory but also to understand the value and importance of each asset in order to prioritise security efforts and protect against potential threats.

A good asset inventory is a foundational piece of a strong ISMS, as properly managed assets are the basis for decisions in risk management, business continuity, and for compliance with laws and regulations like NIS2, DORA, or popular information security frameworks like SOC 2, ISO 27001 and others.

Case Study: The SingHealth Breach – A Lesson in Poor Asset Management

The importance of proper asset inventory management became painfully clear in 2018, when SingHealth - the largest healthcare group in Singapore - suffered a major data breach, compromising 1.5 million patient records, including those of the Prime Minister.

Investigators found that poor IT asset management played a critical role in the breach:

- Unaccounted-for systems left unpatched for over a year were exploited by attackers.
- Weak administrator access controls gave hackers an easy entry point.
- Security teams lacked visibility into all IT assets, delaying detection and response.
- Had SingHealth maintained an accurate, centralized asset inventory, it could have enforced patching, security controls, and monitoring across all systems - potentially preventing the breach altogether.

Sources:

- Committee of Inquiry Report – Ministry of Health Singapore
- Wikipedia: 2018 SingHealth Data Breach

The SingHealth breach is a stark reminder that without a complete asset inventory, security teams can't protect what they don't know exists. But simply understanding the importance of asset management isn't enough - it's time to take action.

If a major healthcare provider can miss critical assets, how sure are you that your organization isn't facing the same hidden risks?

In the next section, we'll break down how to systematically identify, track, and manage assets within your ISMS, ensuring that nothing slips through the cracks.

High Level Process of Asset Inventory Management

To ensure that asset management supports your ISMS, there are several key aspects to focus on. Here's a high-level overview of the process and throughout this in depth guide, I will dive deeper into each of these.

1. Identifying all critical assets is crucial

The first step in effective asset management is identifying all assets within your organisation, including hardware, software, data, and people. This inventory should be regularly updated to reflect any changes, ensuring no critical assets go unaccounted for.

> **Pitfall to avoid**
> Most companies track physical devices but forget about cloud services, SaaS tools, and remote work devices - leaving major security gaps.

2. Classification and categorization based on risk and criticality to support prioritisation

Each asset should be classified based on its criticality and the impact it would have on the organisation if it were compromised. This classification will help prioritise resources, ensuring that the most sensitive and valuable assets receive the highest level of protection.

> **Pitfall to avoid**
> Some organizations create overly complex categories that no one actually uses, while others take a one-size-fits-all approach that doesn't reflect real risks. You should try to get to having orders if not multiple orders of magnitude less number of asset categories than you have individual assets.

3. Every asset must have a clearly defined owner

Every asset should have a clearly defined owner - someone who is responsible for its security, maintenance, and lifecycle management. This helps ensure accountability and prevents assets from being overlooked.

> **Pitfall to avoid**
>
> If ownership is too broad (e.g., just “IT”), there is no clear responsibility and accountability. When assigning owners and managers of assets, try to get as close to a specific person's name as possible, if everyone’s responsible, no-one is. I know, in more modern self-organising flat organisations this is a bit more tricky, but then just try to get to as small of a group of people as possible.

4. Assets must be managed throughout their lifecycle

Managing an asset throughout its lifecycle - from acquisition through use to disposal - is crucial for ensuring security. At every stage of the asset’s life cycle their protection needs need to be assessed, designed and security managed.

> **Pitfall to avoid**
>
> Many organizations fail to retire outdated assets properly. Old software licenses, unused servers, and former employee accounts stay active longer than they should. There’s a few better ways to get into an organisation's infrastructure than an “old” server that is still running somewhere but no-one cares about anymore, so it has all the unpatched outdated software waiting to be exploited.

5. Asset Inventory needs to be kept up to date

Asset management is a dynamic process that requires regular audits and updates to ensure the

accuracy of the inventory. Changes in the organisation's infrastructure, new security risks, or emerging business needs must be reflected in the asset inventory.

> **Pitfall to avoid**
> Treating asset inventory as a one-time task. Without regular updates, records quickly become outdated, creating security gaps and compliance issues.

Why does Asset Management Matter?

A well-managed asset inventory is more than just an operational tool - it's a strategic security foundation. Without a comprehensive and up-to-date view of assets, organizations face blind spots in security, compliance risks, and inefficiencies in risk management.

- Risk Management: find and fix security gaps before they get exploited

A complete asset inventory helps identify vulnerabilities, assess risks, and prioritize security controls. Knowing which assets are most critical allows you to allocate resources efficiently, reducing overall security risk. Without a clear asset inventory, organizations often miss hidden security gaps, leaving systems vulnerable.

- Business Continuity: minimize downtime and recover faster from disruptions

In the event of a disruption or security incident, having an up-to-date asset inventory enables faster recovery. You'll immediately know which assets are essential, allowing you to prioritize them in your business continuity and disaster recovery (BC/DR) plans. Without a reliable asset inventory, organizations waste critical time identifying affected systems, increasing downtime and losses.

- Compliance and Auditing: stay audit-ready and avoid compliance headaches: respond to security incidents faster with full asset visibility

Regulations such as ISO 27001, NIS2, DORA, and SOC 2 require organizations to prove they have a strong asset management process. A well-maintained asset inventory simplifies audits, ensures accurate reporting, and demonstrates that security controls are applied consistently. Without this, compliance efforts become time-consuming and reactive instead of structured and proactive.

- Incident Response: respond to security incidents faster with full asset visibility

During a security breach, knowing what assets exist, where they are, and who is responsible is crucial. A clear asset inventory helps quickly identify compromised systems and contain threats before they spread. Without it, incident response teams are forced to guess, wasting valuable time that could prevent further damage.

- Preventing Shadow IT & Security Blind Spots: eliminate shadow IT and close hidden security loopholes

Untracked assets - whether unofficial SaaS tools, outdated software, or forgotten hardware - can become security risks if they lack proper oversight. A structured asset inventory helps organizations eliminate Shadow IT, ensuring that all systems are accounted for, secured, and managed effectively.

Now that we're all on the same page on why asset management matters, it's time to move beyond the basics and explore how to build a strong, security-focused asset inventory. 🚀

In the next chapters, I'll dive deeper into the practical aspects of implementing and optimising asset management processes. We'll explore how to make your asset inventory more efficient, classify assets to align with your security priorities, and integrate these practices seamlessly into the rest of your ISMS. By doing so, you'll be better equipped to handle the evolving challenges of modern security management while ensuring that every asset remains protected.

How to Effectively Collaborate Within the Organisation to Capture All Assets?

Creating an asset inventory isn't about getting it perfect from day one - it's about ensuring you have a complete and usable list when you need it, whether for audits, risk assessments, or compliance reporting.

Creating a comprehensive asset inventory is not a task that can be completed by the information security manager alone. They will never have enough context to know all the assets or bandwidth to find out.

Your role as the information security manager is to facilitate and coordinate the process, ensuring that all key stakeholders are involved and aligned. You need to involve other people, people that often don't see this as "their job" and "responsibility".

The actual collaboration doesn't need to be rigid or overly formal. Instead of complex hierarchies and frequent meetings, asset inventory collaboration should be efficient, straightforward, and adapted to the organisation's culture. The key is to keep things simple while ensuring everyone involved knows their responsibilities.

Next, a few tips on how to run this collaboration that hopefully set you up for success.

Who should be involved in the Asset Discovery Process?

1. Information Security Manager: Facilitates the process, collaborating with department leads to kick off asset discovery. Rather than micromanaging, the security manager provides guidance and ensures that the right people are involved in the discovery process.
2. Department/Team Leads: Work with the information security manager to identify asset champions within their teams. Department leads ensure that the chosen champions have the appropriate knowledge and access to compile asset information effectively.
3. Asset Champions: Responsible for gathering and logging the relevant asset data for their department. By keeping the process focused on essential information, asset champions ensure that the inventory remains accurate and manageable.

How to Make the Asset Discovery Process a Success with your Stakeholders?

1. **Create Clear and Simple Guidelines for Data Collection**

   Keep things simple by giving each department clear guidelines on what information to collect. Focus on the essentials: asset type, owner, location, and criticality. Avoid overwhelming teams with too many requirements - just gather the information that will help build a solid foundation for security and decision-making.

2. **Use Accessible Tools for Data Collection**

   You don't need complex asset management software at this point. Simple tools like Excel or Notion are more than enough for gathering asset data. These familiar tools let department champions log information quickly and easily in a shared document, making sure everyone can contribute without hassle and keeping the data in one place.

3. **Set a Realistic Timeline for Discovery**

   Set a clear deadline for the initial asset discovery, but keep it realistic. Instead of formal check-ins, let teams work independently while offering support if they need it. A single deadline keeps things moving without putting unnecessary pressure on anyone.

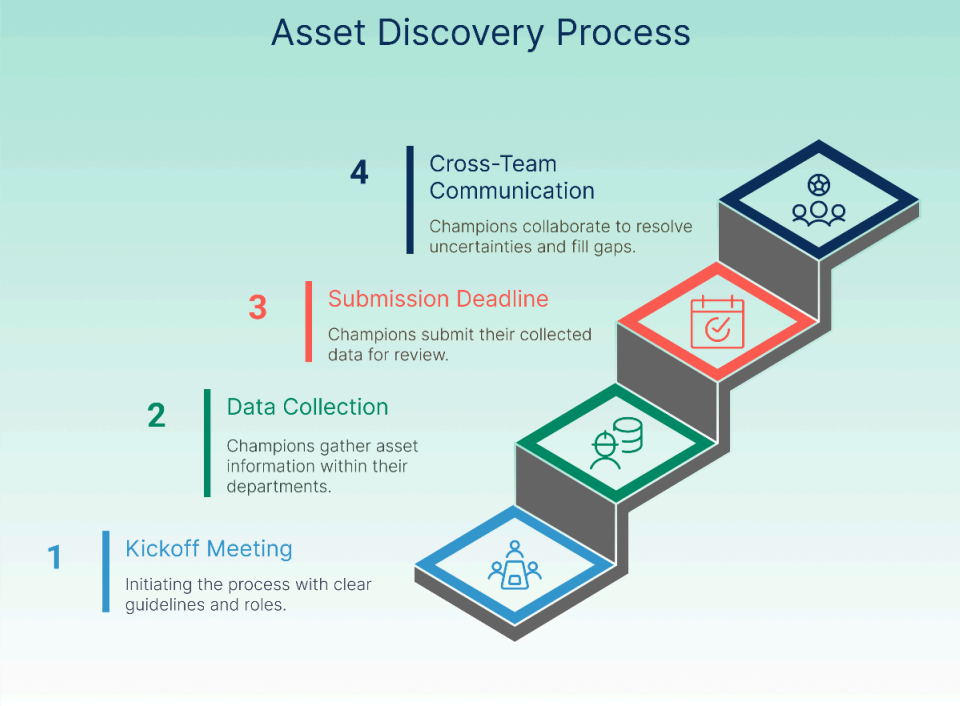
4. **Encourage Informal Cross-Team Communication**

   Asset discovery works best when there's open communication between departments. Encourage champions to reach out to each other informally - quick emails or chat messages are great for getting clarifications or help. This way, teams can collaborate without needing formal meetings.

5. **Focus on High-Value Assets First**

   Start by identifying high-value assets that are critical to your business and security, like core servers, major software platforms, cloud services, and key employee devices. Focusing on these first helps you build a strong foundation, and you can expand to less critical items later as the process continues.

Here's how the initial asset discovery process typically unfolds:



1. Kickoff: The information security manager works with department leads to find asset champions and provide clear guidelines for data collection. The kickoff makes sure everyone knows their role so that the process starts off smoothly. This is the place you share all the prepared material with the champions.
2. Discovery: Asset champions collect asset information for their departments, following the guidelines. They log this information into a shared document or sheet, keeping it simple and accessible. You'll probably need to remind them only 3 times to actually do it.
3. Submission: Champions submit their collected data by the (third) deadline. The information security manager reviews it to ensure everything is complete and follows up on any gaps or inconsistencies.
4. Cross-Team Communication: If there are any uncertainties during discovery, asset champions reach out informally to other departments for clarification or to fill in missing details.

After the initial discovery, the organisation has a solid baseline asset inventory, focusing on high-value assets that are critical to operations and security. This foundation can be expanded as needed, but the first phase keeps things efficient and practical.

What Data Fields Should be Tracked as Part of the Asset Inventory?

When it comes to managing your asset inventory, there is no one-size-fits-all solution. The key is ensuring that you can produce a complete and accurate list of assets when needed - whether for a security audit, risk assessment, or compliance reporting. How you achieve this will depend on your organisation's size, complexity, and the resources available.

Try to avoid starting with buying a new fancy tool for asset tracking. When you're just starting out it's a good idea to start with the tools you already have and over time gain the sense of if you're missing something. In this stage you want your focus to go to asset discovery and not be distracted by a software tool implementation project.

Keep the Core Data Set Minimal

A critical step in managing your asset inventory efficiently is defining the core data that must be tracked for every asset. This involves not only capturing essential details but also categorising assets into meaningful groups based on their type, function, and risk profile. Categorization helps streamline your security efforts and allows you to apply uniform security controls across similar assets, making the process more manageable and scalable within your ISMS.

How to Effectively Categorise Assets?

Categorising assets in an ISMS isn't just about making a list of hardware and software - it's about making security manageable.

Without categorisation, asset management and information security become unmanageable at scale. Trying to define individual security controls for thousands of

unique assets isn't practical, and you would quickly be buried in unnecessary complexity. By grouping assets based on shared security needs and risk levels, organisations can implement controls efficiently, monitor threats more effectively, and maintain oversight as the business grows.

Key Considerations When Categorising Assets for ISMS

A well-structured categorisation system should be based on three primary factors:

1. **Security Relevance** – Assets should be grouped based on how they are protected, rather than just their technical characteristics. For example, laptops used by employees and critical servers running production workloads may both be "hardware," but they require different security controls.
2. **Risk and Impact** – The potential consequences of an asset being compromised should influence how it is categorised. Customer data, financial records, and internal documentation are all information assets, but they are not equally sensitive, and their security requirements will differ.
3. **Business Function** – Grouping assets by how they support business processes helps ensure that security controls align with operational needs. A third-party vendor system used to process customer transactions has a different business impact than an internal knowledge management tool, even if both are SaaS applications. There's a whole section in this guide on how to map assets to business processes.

Common Asset Categories for ISMS

To ensure security controls are applied consistently and efficiently, assets should be grouped in a way that reflects their function and risk profile.

Here are a few commonly used ISMS asset categories:

- End-User Devices & Workstations – Laptops, desktops, and mobile devices used by employees. These assets are endpoints that require encryption, access control, and endpoint security measures.

- Production Systems & Critical Infrastructure – Servers, databases, and cloud environments that host business-critical applications. These assets require strict access management, regular patching, and backup policies.
- Data & Information Assets – Customer records, financial data, internal documentation, and source code. Information assets should be classified based on confidentiality, integrity, and availability requirements to ensure appropriate security controls are applied.
- Identity & Access Management (IAM) Systems – User accounts, authentication systems, and privileged access management tools. These assets control access to critical systems and must be protected with multi-factor authentication, logging, and regular access reviews.
- Third-Party & Cloud Services – SaaS applications, vendor-hosted platforms, and external IT services. These assets introduce supply chain risks and require security reviews, contractual security clauses, and compliance checks.

Common Asset Categorisation Pitfalls and How to Avoid them

A well-structured asset inventory makes security more efficient - but a poorly thought-out categorisation system can create more problems than it solves. The key is to keep categories meaningful without overcomplicating them.

One common mistake is overcategorisation, where organisations create unnecessary subgroups that add complexity without improving security. For example, splitting “End-User Devices” into separate categories for “Marketing Laptops” and “Finance Laptops” doesn’t change how they are secured, but it increases the administrative burden. On the other hand, categories that are too broad - like grouping all “IT Assets” together - can make it harder to apply the right controls.

Another issue is failing to align with actual security and compliance needs. Categorising assets purely by technical type, rather than security impact, can cause gaps. A cloud-based customer database and an internal document management system may both store data, but they have vastly different risk profiles and regulatory requirements.

To avoid these pitfalls, asset categories should be:

- Clear enough to differentiate risk levels but not so detailed that they become unmanageable.
- Aligned with security and compliance requirements so controls can be applied effectively.
- Flexible enough to adapt as the organisation's technology and risks evolve.

The goal of categorisation isn't just organisation - it's making sure security measures are applied efficiently and consistently across all assets.

Example data set for ISO 27011, NIS 2 and DORA compliant asset inventory

To create a truly effective asset inventory, you need to start by aligning the data points you capture with the specific needs of your organisation's risk management, compliance, and security strategies.

Start with the Basics: Keep it Simple Begin by identifying the absolute minimum data that you must track for every asset.

This typically includes:

- Asset Name / Category Unique identifier of an asset or name of the asset group to which the asset belongs, based on similar characteristics, functions, or risk profiles
- Description: Brief summary of the asset, its function, and importance to the organization
- Asset Type: Hardware (laptops, servers), software, data, etc.
- Owner: Who is ultimately accountable for the asset. Making the big decisions.
- Manager: Who is responsible for the day to day maintenance and upkeep of the asset.
- Location: Physical location for hardware or logical location for software/data.
- Status: Is this asset active, retired, or in use? This helps you track lifecycle stages.

Keeping these fields consistent across your entire inventory will ensure clarity, especially when managing diverse types of assets across departments.

Focus on Security and Risk Data Beyond the basics, focus on capturing data that informs your security and risk decisions. Examples of critical data to track might include:

- Criticality: How important is this asset to your organisation's operations? Consider using a simple scale (e.g., high, medium, low) to keep this manageable.
- Access and Permissions: Who has access to this asset? Ensure this data covers both primary and secondary access rights.
- Data Sensitivity: If this asset is a data store, is it confidential, public, or internal? This helps prioritise security controls like encryption.
- Vulnerability Information: Capture whether the asset has known vulnerabilities (e.g., outdated software or unpatched systems).

Tools for Simplifying and Automating Asset Discovery and Monitoring

As your organisation grows, manually tracking assets can become challenging. The good news is that many of the tools your teams already use today likely provide lists of assets automatically - meaning your asset champions don’t need to recall everything from memory. This helps streamline the initial asset inventory process while ensuring your asset inventory stays accurate.

Start with Existing Tools

Begin by leveraging the tools that are already in use across different departments. These tools often have built-in capabilities to track assets, making the initial discovery process easier.

For example:

- HR Systems (like BambooHR or HiBob): These systems track employees and the equipment assigned to them, such as laptops, phones, and access cards.
- IT Systems (like Jira or ServiceNow): These platforms often log hardware, software installations, and support tickets, offering a clear picture of IT-managed assets.
- Procurement Software: Finance or procurement teams likely track purchases and assign them to specific departments or employees, offering a way to account for recently acquired assets.

Using the reports generated by these tools, your asset champions can quickly compile an inventory list based on real data rather than starting from scratch.

For larger organisations or more complex environments, manual tracking and relying solely on department-level tools may not be enough. Here, basic automation can help by automatically discovering devices, software, and networked assets. These tools are especially useful for capturing assets that aren't tracked by typical business systems, such as rogue devices or forgotten software installations.

For example:

- Network Discovery Tools (like Lansweeper): These tools scan your network to detect connected devices and software automatically, creating an ongoing inventory.
- EDR Solutions (like CrowdStrike): Continuously monitor all endpoints and automatically log their status, ensuring that new or previously untracked devices don't go unnoticed.

While automation may not eliminate all manual work, it greatly reduces the chances of missing critical assets, particularly in larger or rapidly changing environments.

Optional Integrations to Keep Your Inventory Current

Once you've established your initial asset inventory, you can consider integrating some of your systems to reduce manual updates. While this step isn't necessary for every organisation, it can be helpful for those looking to streamline updates over time.

For example:

- HR and IT Integrations: When HR systems and IT platforms are connected, changes like new hires or departures automatically trigger updates to the asset inventory, ensuring that issued devices are accurately tracked.

The goal here isn't to replace manual efforts completely but to make the ongoing maintenance of your asset inventory as efficient as possible, especially as your organisation scales.

Common Pitfalls to Avoid when Starting an Asset Inventory

Even when following the best practices, there are ways to implement them incorrectly, leading to inefficiencies or unintended consequences. Below are common pitfalls that arise when building and maintaining an asset inventory - focusing on how things can go wrong even when the right steps are being taken.

1. Overcomplicating Data Collection

While defining a core data set is essential, it's easy to go overboard by collecting too much detail. Overloading teams with unnecessary data points - such as logging every minor attribute or irrelevant detail - can lead to confusion, incomplete records, and frustration among asset champions.

Pitfall

Collecting too much data too early, resulting in inconsistent entries and data management overhead.

How to Avoid

Prioritise only the most critical data points that drive security and compliance decisions. Start simple, and expand only if needed.

2. Setting Unrealistic Expectations for Cross-Team Collaboration

Collaboration is key, but without clear guidelines, it can devolve into a messy, inconsistent process where different teams interpret instructions differently, resulting in poor data quality. Overly rigid or formal collaboration processes can bog down teams, especially in smaller organisations that thrive on agility.

Pitfall

Overly formalising the collaboration process or failing to provide clear, actionable guidance, leading to confusion or lack of alignment.

How to Avoid

Keep collaboration flexible, but provide clear guidelines and focus on outcomes. Make sure teams know what's expected without creating bureaucratic barriers.

3. Over-Reliance on Spreadsheets and Manual Tools

Spreadsheets are a great starting point for collecting data, but they can quickly become unwieldy and prone to errors as the asset inventory grows. Relying too much on manual tools for too long can lead to missed updates, version control issues, or difficulty generating reports when needed.

Pitfall	How to Avoid
Continuing to use spreadsheets when the organisation outgrows them, leading to lost data, inaccuracies, or inability to keep the inventory current.	Gradually transition to dedicated asset management tools or automation solutions as your inventory grows, ensuring your processes scale with your needs

4. Too Much Emphasis on Automation Early On

Automation is useful, but rushing to automate everything without understanding your organisation's unique needs or processes can result in overcomplicated solutions and wasted resources. Automation tools can fail to capture important nuances or require more effort to set up than initially anticipated.

Pitfall	How to Avoid
Overinvesting in automation too early, leading to unnecessary complexity or misaligned workflows that fail to account for manual processes still in place.	Start with basic automation that addresses immediate pain points. Allow manual processes to guide automation development gradually.

With a comprehensive asset inventory in place, you've laid the foundation for stronger security and compliance. But having an accurate list of assets is just the start. In the next chapter, we'll explore how mapping assets to business functions can reveal hidden dependencies and ensure that your security initiatives support operational goals and business continuity.

How to Map Assets to Business Processes?

To protect your business effectively, you need to understand how your assets support its core functions. Having a complete asset inventory is a great start, but it's only part of the picture. The real power lies in mapping those assets to the business processes they enable.

By linking assets to the specific operations they support, your inventory becomes a tool that helps you prioritise resources, manage risks more effectively, and respond faster when things go wrong.

In this chapter, I'll walk you through practical steps to connect your assets to key business processes. You'll learn how to uncover dependencies and integrate this mapping into your ISMS.

Conversations to Uncover Critical Business Processes

Begin by aligning your efforts with the high-level goals of the organisation. Understanding the strategic objectives of your business is critical for pinpointing which processes are indispensable. Ask questions that help you identify the business processes that are essential for generating revenue, maintaining compliance, ensuring customer satisfaction, and supporting internal operations. At this stage, it's important to engage with leadership and department heads to ensure you're focusing on the processes that truly drive the organisation forward. For example, which processes, if disrupted, would cause significant financial loss, regulatory issues, or operational bottlenecks? These are your high-priority areas.

Preparation

- **Prepare Thoroughly:** Before the meetings, review any available documentation on the department's key functions. This will allow you to ask more informed questions and show that you understand the department's responsibilities.

- **Focus on Business Objectives:** Ask questions that uncover the main objectives of the department and how they align with the company's broader goals.
- **Understand Impact:** Get a clear sense of the downstream effects if the process were to be disrupted. This helps in determining the criticality of the process.
- **Map Processes Holistically:** Focus not only on systems but also on people and workflows, as they are integral to how processes function.
- **Avoid Recording Conversations (Unless Appropriate):** While recording discussions might seem like a convenient way to ensure accuracy, it can sometimes make participants feel uneasy or cautious in what they share. Instead, focus on taking detailed notes during the conversation to create a more relaxed atmosphere and encourage openness.
- **Set Expectations in Advance:** Before each meeting, let participants know what the conversation will cover and why it's important. This helps them prepare and ensures they understand how their input contributes to the overall security strategy.
- **Create a Safe Space for Honest Feedback:** Make it clear that the goal of the conversation is not to critique or judge their processes but to better understand how things work and what the potential risks are. Encouraging candidness will help you uncover vulnerabilities or inefficiencies that might not surface in a more formal setting.
- **Be Ready to Adapt on the Fly:** Sometimes, the conversation may take unexpected turns, uncovering new processes or dependencies that were not initially considered. Stay flexible and ready to dig deeper into these areas as they arise.
- **Ask for Practical Examples:** Encourage participants to walk you through real-world examples of how processes function day-to-day. This can help bridge any gaps between how the process is designed to work versus how it actually operates in practice.
- **Follow Up with Clarifications:** After the conversation, review your notes and follow up with any questions or clarifications. This ensures that you fully grasp the details and can accurately map assets to processes.

Example Questions

To ensure your conversations cover all critical aspects of business processes, use targeted questions that help uncover the necessary information. Here are some examples to guide your discussions:

- **Business Objectives:**
  - "What are the top three objectives of your department this year?"
  - "Which processes are critical to achieving these objectives?"
  - "How do these processes support the company's strategic goals, like revenue growth or compliance?"
- **Systems and Dependencies:**
  - "What systems, software, and tools do you rely on most heavily to complete these processes?"
  - "Are there any specific vendors or third-party services that are critical for this process?"
- **Impact of Disruption:**
  - "What would be the immediate and long-term impact if this process were disrupted?"
  - "If a particular system were down for a day, how would that affect your ability to function?"
- **People and Collaboration:**
  - "Who are the key people involved in this process, and how do their roles contribute to its success?"
  - "Which other departments or teams do you collaborate with to ensure this process runs smoothly?"

By combining the detailed insights gained from these walkthroughs with the existing data in your asset inventory, you'll be able to create a comprehensive map that ties each critical business process directly to its supporting assets. Next, let's see what's the process for that.

Linking Assets to Business Processes

With a clear understanding of your critical business processes you can begin the task of linking those processes to the specific assets in your inventory. This step transforms your asset inventory from a simple list of items into a dynamic tool that enhances your ability to manage risks, ensure operational continuity, and align your security strategy with the needs of the business.

By systematically connecting assets to business processes, you'll be able to see how each asset supports the organisation's ability to function, identify areas of vulnerability, and prioritise protection for the most critical systems. Here's how to effectively link your assets to business processes:

Identify Key Process Assets

Go over each business process you have identified. Focus on the key systems, tools, and resources that are identified as essential to those operations to register these in your asset inventory with the mapping back to the process.

Establish Direct and Indirect Asset-Process Links

When mapping assets to business processes, some assets will have an obvious, direct role, while others may support processes more indirectly. It's critical to account for both types of relationships to avoid gaps in your risk management and operational continuity plans. Indirect assets - such as information repositories, key personnel, network infrastructure, or physical devices like printers and security systems - may not be immediately visible in day-to-day operations but are crucial for smooth functioning.

Here are some actionable tips to help you uncover indirect asset-process links:

- Conduct "What-If" Scenarios: During process mapping sessions, ask process owners to consider "what-if" scenarios to expose less obvious dependencies. For example, "What would happen if key personnel were unavailable?" or "If this

document management system were offline, what manual workarounds would be needed?" These questions can reveal indirect dependencies on key assets.

- Review change logs, Incident reports and audit trails: These can be a goldmine for identifying indirect asset links. Look for patterns of activity of assets in different business processes.
- Ask "Who Else Relies on This Asset?": During validation sessions with department heads, ask a straightforward question: "Who else uses this asset, or who would be impacted if it were unavailable?" This is a great open ended question to reveal the hidden dependencies that are often overlooked.

Account for Cross-Department Dependencies

As you map assets to business processes, remember that some assets may serve multiple departments or functions. Identify how processes in one department may depend on assets from another. For example, an HR system may rely on IT infrastructure, or a compliance process may depend on specific data protection systems.

Information Classification

Once you've mapped your assets and started evaluating their role in the organisation, the next step is to classify the information they handle. Information classification helps you determine the level of protection required for each asset based on the sensitivity of the data it processes. This ensures that the right security measures are applied where they're needed most, especially in terms of confidentiality.

The classification process starts by identifying the types of information handled by each asset. Consider whether the asset processes public information, internal records, confidential business data, or highly sensitive and restricted information. Each type of information carries its own level of risk if compromised, which informs how much protection is necessary.

Next, think about the potential impact of unauthorised disclosure or exposure. For public information, the risk is typically low - there's little to no harm if it's made available to others. However, internal information could cause minor disruptions if exposed, while confidential data - such as customer records or financial statements - could result in significant harm.

Restricted information, such as trade secrets or regulated data, carries the highest risk, where exposure could severely damage the organisation, lead to regulatory penalties, or result in legal consequences.

Once you've assessed the sensitivity and impact, classify the information into one of four categories:

- Public: Information that is openly available and not sensitive, with minimal or no impact if exposed.
- Internal: Data meant for internal use that could cause small disruptions if exposed, but does not pose a significant risk.
- Confidential: Sensitive information that could result in substantial harm, such as financial loss or reputational damage, if compromised.
- Restricted: Highly sensitive information that could lead to severe harm, including regulatory penalties or legal action, if disclosed.

Assess the Asset Criticality

Once you've mapped your assets to their respective business processes and classified the information they handle, the next step is to use this information to determine their criticality. This helps you prioritise the security efforts for each asset based on its importance to the organisation, the sensitivity of the information it contains, and the specific risks it faces.

Understanding the criticality of each asset requires evaluating how its failure or compromise would affect different aspects of your organisation - such as operations, finances, legal obligations, and reputation - you can prioritise where to focus your security efforts. This holistic approach ensures that resources are directed to the assets that matter most to the business.

Start by considering the **business impact** of the asset. Think about its role in supporting essential operations. What would happen if the asset was unavailable for a day? Would its failure disrupt core operations, customer service, or productivity? For example, a CRM

system failure might halt sales operations immediately, while the failure of a backup storage system could have a delayed but still significant effect.

Next, consider the financial impact. Some assets are directly tied to revenue, such as a payment processing system, while others might incur recovery costs if unavailable. For instance, an e-commerce website going offline could result in immediate revenue loss, whereas the unavailability of internal project management software might lead to inefficiency but less direct financial consequences. Estimating the financial impact allows you to categorize assets based on the level of potential financial harm - high, medium, or low.

It's also essential to account for compliance and legal risks. Certain assets are linked to regulatory obligations, such as those containing personal data, financial records, or compliance documentation. A failure in a financial reporting system during a regulatory audit, for example, could result in fines or legal action. Identifying assets with regulatory ties helps you understand the potential legal consequences of their failure and assess their criticality relative to those risks.

Consider the reputational impact as well. Could the failure of an asset erode customer trust, damage your brand, or expose your organisation to negative publicity? A data breach involving customer information, for instance, could have serious reputational damage, potentially even more than the financial loss incurred. Assess the reputational risks and rate them accordingly.

Another factor to evaluate is the recovery difficulty. Some assets are easier to recover than others. Restoring a database from backup might be straightforward, but rebuilding a custom application server could take days or weeks. The time and complexity involved in restoring an asset can influence how critical it is to the organisation's operations.

Once you've gathered this information, you can assign a Criticality Rating to each asset taking all this information into account. This rating reflects the overall importance of the asset to your organisation, factoring in its business, financial, compliance, reputational, and recovery implications. For example, you might use a rating system where high-criticality assets are those whose failure would cause severe disruption or damage, medium-criticality assets would lead to moderate impact, and low-criticality assets would have minimal or no significant effect on operations.

Validate and Refine with Stakeholders

Once you have gathered all this information. Review the asset-to-process mappings and criticality assessments with stakeholders to confirm that all relevant assets have been properly linked. Use their feedback to refine your inventory and fill in any gaps.

Maintain and Update Regularly

As with the asset registry itself, also the asset-to-process mapping is not a one-time activity. As business processes evolve, new assets are added, and others are retired, it’s important to continuously update your mappings. Regularly review and refine the connections between assets and processes as part of your ISMS to ensure that your security strategy remains aligned with the organisation’s needs.

Common Pitfalls and How to Avoid Them

Even with a well-structured approach, there are several ways the process of linking assets to business processes can go awry. It's not just about completing the steps but doing them effectively. Below are common pitfalls that can arise during the mapping process and tips on how to avoid these issues to ensure your asset-to-process connections are accurate and actionable.

1. Overcomplicating the Mapping Process

Pitfall	How to Avoid
Attempting to map every single asset to all possible business processes can lead to an unnecessarily complex and confusing asset-to-process map. This can overwhelm teams and make it difficult to identify the truly critical connections.	Focus on mapping only the most critical assets that have a significant impact on each process. Prioritise the assets that, if compromised, would have a clear negative effect on the business.

2. Over-reliance on Departmental Silos

Pitfall

It might be easy to rely heavily on individual department input without considering how assets span across different departments or processes. This can lead to fragmented mappings where cross-functional assets are overlooked or misassigned.

How to Avoid

Actively involve cross-departmental collaboration when identifying assets that serve multiple business units. Make sure to map these shared assets to all relevant processes to ensure comprehensive coverage.

Mapping your assets to critical business processes is a vital step in transforming your asset inventory into a dynamic tool that enhances operational resilience and strategic decision-making. By clearly understanding how each asset contributes to the overall functioning of your organization, you can better manage risks, prioritize resources, and respond effectively to incidents. However, this process doesn't end here - it's an ongoing effort that evolves alongside your business. In the next chapter, we'll explore how assigning clear ownership and custodianship to each asset ensures accountability, keeps your asset management strategy agile, and maintains the integrity of your ISMS as your organisation grows and changes.

How to Find and Assign Owners and Custodians/Managers for Assets?

Assigning clear ownership and custodianship for your assets is key to making your asset management system work smoothly. Think of ownership as assigning responsibility: someone who's accountable for each asset's security, usage, and lifecycle. Custodianship, on the other hand, involves the day-to-day management of that asset, ensuring it's maintained and operating securely.

Why does this matter? Because when ownership is vague, security gaps emerge, and assets slip through the cracks. If everyone is responsible, then no one is truly accountable, leading to confusion and neglected assets. Knowing exactly who's responsible for every asset - from laptops to critical data systems - ensures that nothing is overlooked.

Ownership also drives accountability, which is crucial for making sure assets are protected, regularly updated, and properly decommissioned when their lifecycle ends. In this section, we'll explore how assigning the right people to the right assets strengthens your asset management practices, supports compliance, and keeps your organisation secure. You'll learn how ownership and custodianship are two sides of the same coin - both critical to keeping assets secure and well-managed across their entire lifecycle.

Difference Between Asset Owners and Asset Custodians

When you have the right people overseeing your assets, nothing falls through the cracks. Next we'll look into how to effectively designate owners and custodians for all assets in a way that aligns with your operational and security goals. But first, we need to be on the same page on the definitions.

Owners

The owner is usually the person or team with the most to gain (or lose) from the asset. They're the ones who are accountable for making sure the asset continues to deliver value for the business. Owners are focused on the bigger picture - they make decisions about how the asset aligns with business goals, keeps things secure, and ultimately serves the organisation's long-term strategy.

- **Strategic Responsibility:** The owner is responsible for the high-level decisions, like whether the asset should be upgraded, replaced, or retired. Their job is to make sure that the asset helps the company achieve its objectives, whether that's boosting revenue, improving customer relationships, or staying compliant with regulations. For example, a marketing director might be the owner of a CRM system because it's key to managing customer relationships and driving sales.
- **Financial Responsibility:** Owners often manage the budget related to the asset, ensuring that the investment delivers a return. They decide on purchases, upgrades, and necessary maintenance, keeping the asset aligned with the organisation's priorities while staying within budget constraints.

Custodians

The custodian is responsible for the asset's day-to-day operations and maintenance, ensuring it functions efficiently and securely. While owners focus on the strategic value, custodians take care of the operational health, keeping everything running smoothly.

- **Day-to-Day Management:** Custodians manage the details that keep the asset running efficiently. Whether it's ensuring physical equipment like security cameras are regularly serviced, updating software, or keeping sensitive data properly stored, they handle the nuts and bolts. For example, an HR professional could be the custodian of employee records, ensuring they're accurate, updated, and securely maintained in accordance with privacy laws.

- **Operational Security:** Custodians are on the front lines of safeguarding assets, whether that means ensuring physical security measures for office buildings, applying encryption to data repositories, or managing access controls for sensitive information. A facilities manager, for example, might ensure that building security systems are operational and properly secured, while a legal custodian might protect intellectual property by managing access to confidential documents.
- **Compliance and Maintenance:** Custodians play a critical role in maintaining compliance with both internal policies and external regulations. This can range from making sure that medical equipment is calibrated and meets health standards, to ensuring that financial records comply with audit requirements, or even maintaining up-to-date software licences. Custodians also handle ongoing maintenance, whether that's running regular checks on equipment or keeping digital assets secure and compliant.

By separating ownership and custodianship, you can streamline management while ensuring that strategic oversight and practical maintenance are both covered.

How to Identify the Right Asset Owners

Start with the business outcomes and business processes

Each department or function within the organization is responsible for certain outcomes - whether it's revenue generation, customer satisfaction, compliance, or internal operations. The asset owner should be the person or team most directly responsible for these outcomes as they relate to the assets in question.

Evaluate decision-making authority The asset owner should have the authority to make high-level decisions about the asset's use, maintenance, and lifecycle. This includes decisions about upgrades, replacements, or decommissioning. Consider who has the decision-making power for investments related to the asset and who is responsible for ensuring that the asset continues to deliver value to the organisation. This will help you identify the most appropriate owner.

Assess Accountability for Risk Identify who is accountable for the risks associated with each asset. For example, if the asset fails or becomes compromised, who would be responsible for the business impact? The owner should be someone who is able to manage that risk and is invested in mitigating any potential disruptions. This means they must be in a position to not only ensure the asset's operational continuity but also assess and address risks proactively.

Maintain Flexibility for Organisational Changes Businesses are dynamic, and roles can shift over time. Be prepared to revisit asset ownership as organisational structures change or new roles emerge. Regular reviews can help ensure that ownership is kept up-to-date and reflective of any changes in business priorities or personnel.

How to Identify the Right Custodians

In a perfect world, the asset owner and custodian would be the same person - it would simplify everything. However, the reality is that many assets require specialised day-to-day management that goes beyond the scope of the owner's responsibilities and skill set.

Ask the Asset Owners

Identifying the right custodian for each asset starts with a conversation. Often, the simplest approach is to begin with the asset owner. Since owners are responsible for the strategic direction and overall value of the asset, they're typically well-positioned to help identify the person or team who manages its day-to-day operations. Ask the owner questions like:

- "Where do you turn when there's an issue with this asset?"
- "Who is responsible for keeping this asset up and running?"
- "Who performs regular maintenance, updates, or troubleshooting?"

These questions will often lead you directly to the people who already have their hands on the asset and are familiar with its operational needs.

Match Skills to Responsibilities

Once you've identified potential custodians through discussions with the owner, evaluate whether they have the necessary skills to manage the asset effectively. It's not just about who currently touches the asset; it's about ensuring that the custodian has the right technical abilities or specialised knowledge to meet the demands of the asset, whether it's managing a physical piece of equipment, overseeing software, or handling sensitive data.

Ensuring Role Clarity and Commitment

Once you've identified the right owners and custodians for each asset, the next step is ensuring they fully understand and accept their roles. Simply assigning responsibility is not enough; you need to make sure that those tasked with ownership and custodianship are clear on their responsibilities and committed to fulfilling them.

Hold Clear Conversations to Establish Role Clarity

It's essential to have direct and transparent conversations with both owners and custodians. These discussions should cover:

- What their responsibilities entail: Clearly define what it means to be an owner or custodian. For owners, this might include strategic decision-making, managing risks, and ensuring the asset's alignment with business goals. For custodians, this will focus on operational tasks such as maintenance, security, and compliance.
- Why their role is crucial: Help them see the bigger picture - why their role is key to keeping the organization secure and ensuring smooth operations. This also reinforces accountability.
- What success looks like: Outline what you expect in terms of performance. For example, custodians should be aware of how frequently assets need to be checked, maintained, or updated, and owners should understand the importance of regular reviews and decision-making.

Document the Responsibilities

Put the roles and responsibilities into writing. Formalising ownership and custodianship roles helps prevent misunderstandings and ensures accountability.

Common pitfalls and how to avoid them

Even when following best practices, there are ways to misstep when assigning ownership and custodianship. Let's look at a few common pitfalls and how to avoid them.

1. Assigning Ownership Without Real Accountability

Pitfall

You've designated someone as the asset owner, but they don't have the authority or responsibility to make real decisions.

The title of "owner" is there, but they're not empowered to manage the asset's budget, make critical lifecycle decisions, or mitigate risks.

How to Avoid

Ensure that the person you designate as an owner has real authority over the asset. If they can't make strategic decisions about the asset, they aren't the right owner.

Revisit whether they have the budget control, decision-making power, and access to the right resources to effectively manage the asset. If not, consider who else is better positioned to hold that responsibility.

2. Overlapping or Conflicting Roles

Pitfall

You assign an asset to multiple owners or custodians without clearly defining where their responsibilities begin and end. This leads to confusion, with tasks falling through the cracks or, worse, conflicting actions being taken.

How to Avoid

Clearly delineate responsibilities. If more than one person is involved, make sure their roles are complementary and not overlapping. For example, you might have a primary owner responsible for strategic decisions and a secondary owner for budget oversight, but ensure they both understand their distinct roles.

3. Overloading One Person with Too Many Assets

Pitfall

You've done a great job assigning owners and custodians but accidentally overloaded one person with too many assets to manage effectively. This spreads their attention thin, resulting in neglected responsibilities.

How to Avoid

Take a balanced approach when assigning roles. Regularly assess the workload of each owner and custodian to ensure no one is overburdened. If someone is managing too many assets, consider redistributing some of those responsibilities to avoid burnout and ensure proper management across the board.

4. Defaulting to the Highest-Ranking Person as the Owner

Pitfall

It’s tempting to assign the highest-ranking person in a department, like the CTO or CFO, as the owner of every asset under their jurisdiction. While this might seem convenient, it often results in ineffective ownership. Senior leaders are responsible for the overall strategy, but they may not have the time or detailed knowledge to ensure that specific assets are optimally managed and aligned with operational goals.

How to avoid

Assign ownership based on proximity to the asset's day-to-day strategic importance rather than rank. For example, instead of making the CTO the owner of every IT system, it might be more effective to assign ownership of critical applications to the department heads or managers who work closely with those systems and understand their role in achieving business outcomes. The CTO can still provide oversight for high-level strategy without being burdened with ownership of every individual asset. This approach ensures that ownership is meaningful, actionable, and better aligned with the asset's specific use and value.

With a comprehensive asset inventory in place, each asset now mapped to critical business processes and assigned both an owner and a custodian, you’ve established a solid foundation for managing your organisation's key resources. But managing assets doesn’t end with assigning responsibilities. Every asset has a lifecycle - from acquisition and operational use to updates and eventual disposal - and each phase requires attention to maintain security, compliance, and operational efficiency.

In the next chapter, we'll dive into how to effectively manage assets at every point in their lifecycle. From acquisition and updates to secure disposal, we'll explore practical steps you can take to ensure that your assets remain secure and well-managed from start to finish.

Asset Lifecycle Management

In asset management, your job isn't done once assets are inventoried and assigned. Every asset, whether digital or physical, follows a lifecycle - from acquisition to disposal - and managing each stage is essential for maintaining security, compliance, and operational efficiency. This chapter will walk you through practical steps to ensure that every asset remains secure throughout its entire lifecycle.

Acquisition

When assets enter the organisation, whether through purchase, development, or internal creation, it's important to integrate into the asset registry. For this we follow the foundational steps we've already covered - categorising, classifying the asset and assigning the appropriate owner and custodian

Operational Use

Once an asset is in use, it begins delivering value to the organization.The asset custodian plays a key role here, managing day-to-day operations, while the asset owner ensures that the asset continues to support the organisation's broader goals.

Maintenance and Updates

As assets age, they require ongoing maintenance and updates to stay secure and functional. This stage also involves reassessing the asset's classification and risk profile, as its use or criticality may have changed. Both the asset custodian and information security manager must ensure that these updates are carried out effectively, with the asset owner overseeing strategic decisions about potential upgrades or continued use.

Decommissioning and Disposal

Eventually, assets reach the end of their useful life and must be decommissioned. Secure disposal is critical to prevent any potential security breaches. The information security

manager ensures that disposal processes comply with regulations, the asset custodian handles the execution of secure disposal, and the asset owner oversees the overall process, confirming that the asset is no longer required for business operations.

Why Understanding the Unique Lifecycle of Each Asset is Important?

While it's useful to define the generic lifecycle stages of an asset - acquisition, operational use, maintenance, and disposal - this framework alone isn't enough to fully secure and manage each asset. Discovering the **unique lifecycle** of each asset provides critical insights that inform key decisions and strategies for security, compliance, and resource allocation.

Here's why this understanding matters:

Tailored Security Controls

Each asset type has its own risks and requires specific security controls. For instance, customer data might need encryption and strict retention policies, while a laptop requires regular updates and secure access. Understanding the asset's lifecycle helps tailor security measures at each stage to match its risk profile.

Compliance Alignment

Certain assets are subject to specific regulatory requirements. For example, medical records may have strict retention rules, and servers might need certified destruction. Knowing the lifecycle ensures compliance at every stage, helping to avoid legal risks.

Strategic Resource Allocation

Understanding an asset's lifecycle helps allocate resources efficiently. Long-term assets like IT systems need regular monitoring and updates, while short-lived assets like documents require quicker disposal. This knowledge ensures critical assets get the attention they need.

Informed Strategic Decisions

A clear understanding of an asset's lifecycle allows the owner to make informed decisions

about upgrades, replacements, or decommissioning. For example, retiring outdated software or replacing worn-out equipment ensures assets continue to meet business goals while minimising risk.

Uncovering the Unique Lifecycle of Each Asset

Engage with Stakeholders to Understand the Asset's Purpose

Begin by consulting the asset owner and custodian to identify the core purpose of the asset, its expected usage, and strategic significance. These conversations help clarify the asset's value to the business, operational demands, and potential risks, providing a foundation for uncovering its specific lifecycle.

Map the Expected Stages

Based on input from stakeholders, outline the specific lifecycle stages for the asset - acquisition, operational use, maintenance, and disposal. This helps clarify the timeline and actions needed at each phase, as well as the security controls that should be applied.

Leverage Historical Data

Where applicable, look at similar assets used in the past to estimate the lifecycle more accurately. This data helps predict operational durations, update cycles, and disposal timelines, guiding more informed decisions.

Plan for Exceptions

Finally, identify any potential deviations from the standard lifecycle. Whether its extended retention for legal reasons or special disposal requirements for certain assets, planning for exceptions ensures that all assets remain secure and compliant, regardless of their lifecycle variations.

With a good understanding of the unique lifecycle our assets go through, we can now focus on the next critical step: designing the specific security controls needed for each asset.

Common Pitfalls and How to Avoid Them

Now that you have a comprehensive understanding of the assets in your inventory - how they are mapped to business processes, their criticality, and the unique stages of their lifecycle - you have the key information needed to start designing security controls tailored to each asset. In the next chapter, we'll explore how to create effective security controls that align with each stage of the asset lifecycle, ensuring that your assets are protected from acquisition through to decommissioning.

Assessing Security Needs of Each Asset

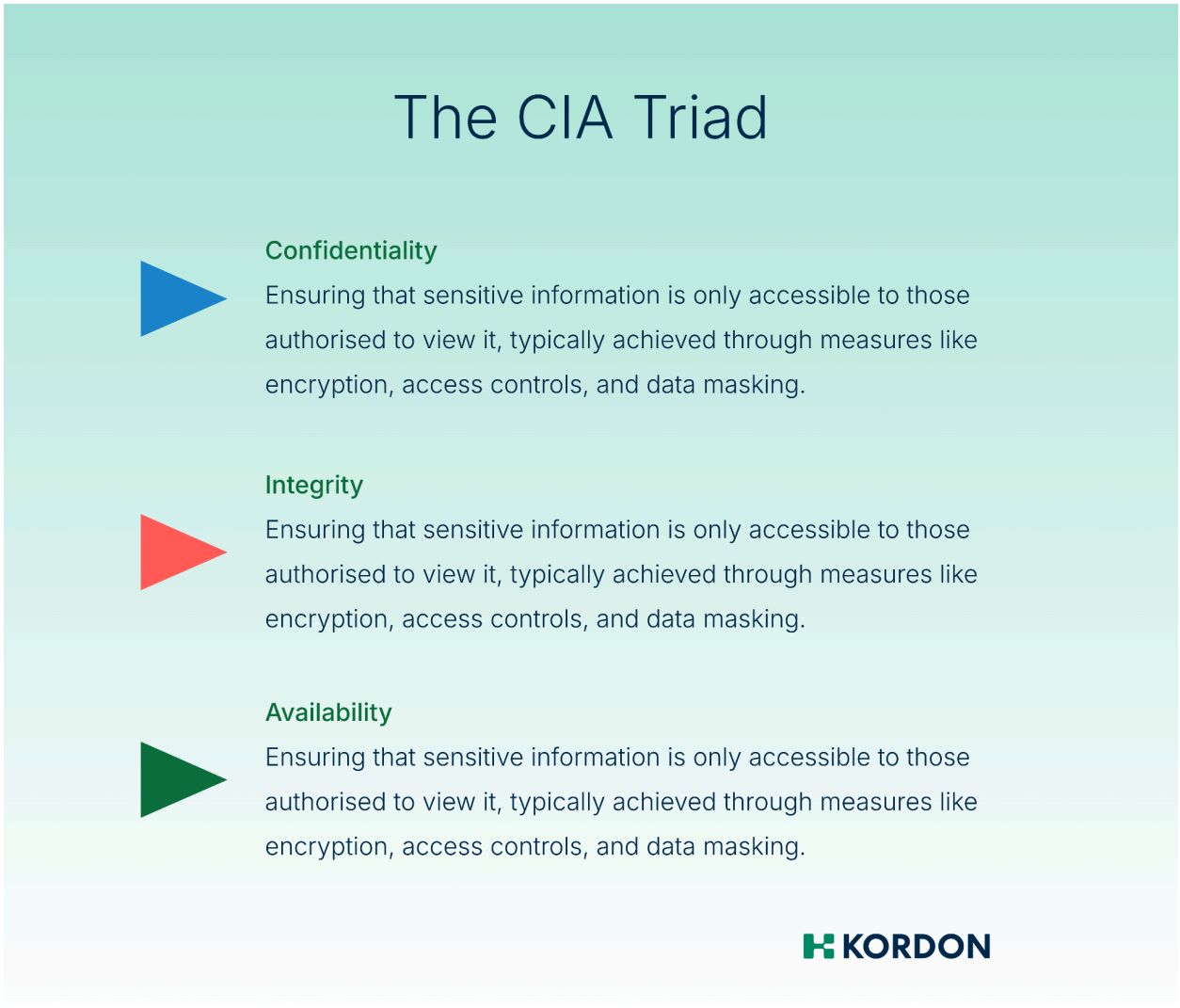
Before we can design effective security controls for each asset, we need to understand their specific security needs. This involves taking into account both internal information - such as the assets criticality, and the confidentiality, integrity and availability needs (CIA Triad) for information assets - and external factors, such as the threats the asset may face and the risks associated with those threats materialising.

This chapter will guide you through assessing the security needs of each asset, focusing on how to align the CIA Triad - Confidentiality, Integrity, and Availability - with the asset's criticality and lifecycle stage. We will also briefly address external risks and threats that could impact the asset. This book focuses on the asset management piece of this equation, so we won't go too deep into risk assessment methodologies.

The CIA Triad

The CIA Triad is a foundational model in information security that represents three key principles necessary for protecting assets:

- Confidentiality: Ensuring that sensitive information is only accessible to those authorised to view it, typically achieved through measures like encryption, access controls, and data masking.
- Integrity: Ensuring that data remains accurate, unaltered, and trustworthy throughout its lifecycle. Integrity is maintained through methods like checksums, digital signatures, and version control to prevent unauthorised modifications.
- Availability: Ensuring that information and resources are accessible when needed by authorised users. This is achieved through redundancy, backup systems, and disaster recovery plans to ensure that critical systems remain operational.



We assess each asset's needs in each of these categories - confidentiality, integrity, and availability - to determine the level of protection required throughout its lifecycle and design tailored security controls accordingly.

Assessment methodologies

When you have multiple assets with varying levels of criticality, confidentiality, integrity, and availability (CIA) ratings, comparing and prioritising them can become complex due to the multi-dimensional nature of their protection needs. To simplify this, there are a few practical approaches you can follow, ranging from simpler valuation methods to more structured risk and security prioritisation techniques.

Asset Value-Based Approaches

The simplest way to prioritise asset protection is by evaluating the inherent value of each asset itself, rather than just the impact of its compromise. This approach works particularly well for physical assets.

- What It Is: Assign a value to each asset based on factors like replacement cost, downtime cost, or potential loss of intellectual property. The value could be quantified in monetary terms or categorised using a simple rating system like low, medium, or high.
- How It Works: Assess the inherent value of each asset and categorise it accordingly. For instance, a critical server may be rated as high-value due to significant replacement costs and the operational impact of downtime, while a peripheral device like a printer could be rated low-value due to its minimal impact if lost or compromised.
- Prioritisation: High-value assets - those with significant replacement costs, operational impact, or a high-value rating - are prioritised for more rigorous protection. This approach is straightforward and effective for physical infrastructure or assets with clear financial or operational implications, ensuring that valuable assets receive the protection they deserve.

Weighted Scoring System

For a more detailed analysis, especially when dealing with information assets and considering multiple protection needs, a weighted scoring system offers a balanced approach.

Step 1: Assign weights to each of the four factors - Criticality, Confidentiality, Integrity, and Availability - based on their importance to your organization.

Factor	Weight (%)
Criticality	40%
Confidentiality	20%
Integrity	20%
Availability	20%

Step 2: Rate each asset on a consistent scale for the four factors (e.g., 1 to 5, where 5 is high and 1 is low).

Step 3: Multiply each score by its respective weight and sum the results to get an overall score for each asset.

Asset	Criticality	Confidentiality	Integrity	Availability	Weighted Total Score
Asset 1	5 * 0.40 = 2.0	4 * 0.20 = 0.8	3 * 0.20 = 0.6	3 * 0.20 = 0.6	4.0
Asset 2	3 * 0.40 = 1.2	5 * 0.20 = 1.0	4 * 0.20 = 0.8	4 * 0.20 = 0.8	3.8

Working with arbitrary values like 4.1 and 2.8 day to day can become tedious. This is why you might consider introducing a priority tier concept to this like in one of the following approaches.

Assign Priority Tiers

If you prefer simplicity, categorising assets into priority tiers based on their scores can help you streamline decision-making and allocate resources more effectively. This approach groups assets into tiers, reflecting their relative importance to the organisation based on criticality and the CIA (Confidentiality, Integrity, Availability) factors.

- Tier 1 (Highest Priority): Assets with high criticality and at least one high score in confidentiality, integrity, or availability. These assets require immediate attention and the strongest security measures, as their compromise could cause significant operational, financial, or reputational harm.
- Tier 2: Assets with medium criticality and medium-to-high scores in one or more of the CIA factors. These assets still play an important role in the organisation but pose less of a risk than Tier 1 assets. They need moderate security controls.

- Tier 3 (Lowest Priority): Assets with low criticality or consistently lower scores across confidentiality, integrity, and availability. These assets, while still important, pose the least risk and require less stringent security controls.

This tier-based approach helps to group assets based on overall risk and importance, making it easier to prioritise security efforts and allocate resources more efficiently.

Example:

Let's consider three assets with the following scores for Criticality, Confidentiality, Integrity, and Availability:

Asset	Criticality	Confidentiality	Integrity	Availability	Tier
Asset 1	5 (High)	4 (High)	4 (High)	3 (Medium)	1
Asset 2	3 (Medium)	5 (High)	3 (Medium)	4 (High)	2
Asset 3	2 (Low)	2 (Low)	2 (Low)	3 (Medium)	3

Risk Assessment

While this book focuses on asset management and its role in informing security controls, it's important to acknowledge that risk management plays a significant part in shaping your overall security strategy. Ultimately, when designing and implementing controls to protect your assets, risk assessment helps identify potential threats and vulnerabilities, and determines how likely these risks are to materialize and what their impact might be.

However, this book focuses on asset management and will not delve into the details of risk assessment for designing risk mitigation controls. Risk assessment is a broader, more complex discipline, worthy of its own book.

Designing Security Controls

Once your asset inventory is in place and the security needs of each asset have been assessed, the next step is ensuring those assets are protected throughout every phase of their lifecycle. From acquisition to disposal, each stage presents unique requirements that must be supported by well-designed security controls. As an information security manager, your role is to facilitate the creation of these controls by ensuring that the right processes are followed and that the security needs of the assets are properly addressed.

In this chapter, we'll explore how you, as an information security manager, can guide the development of security controls for assets across their lifecycle. This includes collaborating with asset custodians who have the necessary expertise to design these controls and validating that the measures in place align with both the asset's lifecycle stage and the overall security objectives of the organization.

Who Designs the Controls?

As an information security manager, while you're deeply involved in creating many foundational controls - like information security policies, access management, and compliance-related controls - you're not expected to design all the security controls yourself. That's where asset custodians come in. These experts know the ins and outs of each asset they manage and are best equipped to develop the specific controls these assets need. Your role, however, remains critical. You're responsible for facilitating and coordinating this process, ensuring that the controls custodians create align with your organization's broader security strategy.

Establishing Trust and Feedback Loops

Trust is foundational to effective collaboration with custodians. When custodians feel empowered and trusted, they are more likely to contribute meaningfully to the control design process. This means not just allowing custodians to participate, but actively valuing their insights. Their knowledge of the specific technical, operational, and contextual aspects of each asset helps ensure that the controls they design are appropriate and realistic. If custodians perceive that their input is respected and taken seriously, they are more likely to take ownership of the controls, seeing them as their responsibility rather than a mandate handed down from above.

Trust also facilitates honest conversations about potential challenges or limitations in the control design. Custodians should feel comfortable pointing out when a control is impractical or doesn't fully address the risks associated with an asset. This can be particularly important when dealing with complex assets that may not fit neatly into existing security frameworks, or when controls must balance security with business functionality. A trusting relationship ensures that custodians feel safe to voice concerns early, allowing for better problem-solving and stronger, more effective controls.

Establishing trust is not a one-time event; it's an ongoing process that requires consistent and open communication. As the information security manager, fostering this environment means encouraging custodians to actively share their insights while also being receptive to their feedback. Trust creates a collaborative culture where custodians are partners in security, not just implementers of controls.

Discovering What Already Exists

Before diving into designing new controls from scratch, a crucial step in the process is uncovering what security measures are already in place. These measures often fall into two categories: centralised security processes and informal operational practices. Centralized security processes, such as vendor reviews, user access management, or incident response protocols, are typically established at an organizational level and apply universally across multiple assets. These processes are critical baseline controls for each asset lifecycle stage that reduce the need for redundant control design across different assets.

In addition to these centralised processes, many assets are already protected by informal security measures - operational practices that aren't officially labeled as "security controls" but nonetheless provide a layer of protection. Examples might include informal access restrictions, regular data backups, or equipment maintenance routines. These existing practices can serve as valuable building blocks when formalising security controls for your assets.

By recognizing both the centralised processes and the informal operational practices that already exist, custodians can focus on filling in the gaps and enhancing these measures to create a more structured, formal control environment.

Toolset for Control Designers

Once there's an understanding of what baseline security processes exist, it's time to start designing asset specific security controls.

This process should start by mapping out what implicit security controls are already in place at different asset lifecycle stages and where the gaps are.

Example Supportive Documentation

One way you the information security manager can help custodians in this process process is with a set of templates, and guidelines. When sharing this documentation make sure to highlight the iterative nature of controls and the importance of recognising different security needs an asset might have in its different lifecycle stages. One great way to do this is by sharing examples of controls at different maturity levels and for different lifecycle stages. Perfection is the enemy of progress, it's more important to start with something than to wait until the preparation for perfection is complete.

- Guiding principles for asset custodians

This document is designed to introduce new asset custodians to their role within the organisation's security framework. It outlines the expectations for asset custodians, including their responsibility to design, implement, and manage security controls that protect the assets they oversee. The document provides context on why these controls are necessary, emphasising the regulatory, compliance, and organisational requirements that drive security policies.

Additionally, this guide offers principles to help custodians design effective controls, focusing on key factors such as confidentiality, integrity, and availability (CIA triad). It provides practical examples of what to consider when creating controls, such as potential risks, access management, data protection, and the alignment of controls with broader compliance objectives like ISO 27001 or SOC 2.

This document also serves as a reminder that custodians are not working in isolation - rather, they are part of a broader security ecosystem, and their role is integral to the organization’s overall information security management system (ISMS).

- Guiding questions to discover implicit “hidden” controls that are already in place

This document helps custodians uncover existing security measures that may not be officially documented but are already serving as controls. The guiding questions prompt custodians to think critically about operational practices that safeguard the asset. Example questions might include:

- How is access to the asset restricted and monitored?
- What steps are taken to ensure the accuracy of the data?
- How do you ensure that systems remain operational during peak periods?

This document helps custodians identify "hidden" controls that can serve as a starting point for formalising their security measures.

- Control template

The control design template provides custodians with a standardized format to document security controls. It includes sections for:

    - Objective: What is the control intended to achieve?
    - Scope: Which assets or systems does this control apply to?
    - Control Description: Detailed explanation of the control.
    - Implementation Steps: A step-by-step guide to implementing the control.
    - Monitoring and Maintenance: How the control will be monitored and maintained over time. This template ensures that controls are consistently documented across the organisation, while also allowing flexibility to adapt to specific asset needs.
- Risk assessment template

This template guides custodians through a structured process for assessing the risks associated with their assets. It includes fields for identifying potential threats, vulnerabilities, and the impact of security breaches. The risk assessment template prompts custodians to evaluate the likelihood of these risks materialising and prioritise their control design accordingly. By aligning controls with the risks identified, custodians can ensure that their efforts are focused on the most critical areas, helping to mitigate potential security gaps effectively.

With this chapter the journey has gotten us from mapping out the assets the organisation has to understand their security needs and designing appropriate security controls. Amateurs might say that we are done, but others will know, that this is just the beginning, now we need to operationalise this process to be ever running, adapting to the changes in the business, environment and the assets themselves. The next few chapters will look into how to bring the basic minimal asset management process we have set in place to the next level.

Keeping Your Asset Inventory Current

Once your asset inventory is established, the real challenge begins: keeping it accurate and up-to-date. An outdated or incomplete asset inventory can leave your organisation vulnerable, making it harder to protect critical assets, manage risks, or meet compliance requirements. Asset management isn't a one-time task - it's a continuous process that evolves alongside your organisation's operations, technology, and environment.

In this chapter, I'll dive into why maintaining a current asset inventory is so crucial and how you can make it happen without bogging down your teams. I'll explore practical ways to stay on top of your inventory through regular audits, smart automation, and proactive management. You'll learn how to schedule reviews, automate updates where it makes sense, and uncover those hidden risks from untracked assets - like Shadow IT. The goal? Keep your inventory accurate, actionable, and easy to manage so that it remains a powerful tool for protecting your organisation, not just a box to tick off.

Regular Audits

Asset inventory auditing builds on the foundations of the asset inventory process you've already put in place. While the initial phases of asset management - like discovery, classification, and assignment - help establish a solid inventory, regular auditing is the process that ensures this foundation remains reliable over time. It's the mechanism by which you catch changes, updates, and the inevitable shifts that occur as your organisation grows and evolves.

This section will walk you through how to establish an audit routine that fits into your workflow without becoming a burden. By setting a clear schedule, using effective checklists, and involving the right stakeholders, you'll ensure that your asset inventory

continues to serve its purpose as a dynamic tool for managing security, risk, and compliance.

Setting the Audit Scope

Ultimately, the goal of asset auditing is to ensure that all assets are regularly reviewed and that every dimension of your asset inventory is fully accounted for. This means verifying not just the existence of each asset but ensuring that the data is accurate, assets are properly classified, and ownership is clearly assigned. To make this process manageable, each audit cycle can focus on specific objectives, such as uncovering any shadow IT that has emerged since the last review or confirming that decommissioned assets have been fully removed from operational systems. These objectives help ensure that audits remain targeted and produce actionable results while working towards the broader goal of maintaining a complete and accurate asset inventory.

It's important to note that while asset data is also often audited together with the controls associated with each asset, this book remains focused on the asset management side of things. To make sure that when you are auditing the controls, you know that you have all the assets accounted for. Therefore, I will not dive into how to audit whether the controls implemented around an asset are functioning properly or meet the security requirements outlined in your ISMS, ensuring the accuracy and completeness of your asset inventory itself, leaving the control audits to be covered by broader ISMS compliance efforts.

Here’s a suggested order for prioritising assets for audits, which allows you to stagger the workload and optimise resources. Coincidentally this list should work both for auditing the asset inventory and the asset controls.

Priority 1: Critical Assets

Start by auditing assets that have been classified as high criticality or essential to business operations. These assets have the most significant impact on your organisation’s operations, finances, or compliance. For example, production servers or customer data repositories should be prioritised because their compromise could severely disrupt

operations or result in regulatory penalties. Audits for these assets should be conducted quarterly or even more frequently if required.

Priority 2: Assets Flagged in Previous Audits

Next, focus on assets that were flagged in previous audits for issues such as outdated information, misclassification, or vulnerabilities. These assets require follow-up to ensure that the problems identified in prior audits have been addressed. For instance, if a software system was flagged due to outdated security controls, it's essential to confirm that the necessary corrective actions have been implemented. Audits of unresolved issues should occur quarterly, with resolved issues tracked semi-annually.

Priority 3: High-Change Assets

Afterwards, turn your attention to assets that experience frequent updates, changes, or turnover. This includes items like employee laptops, cloud services, or vendor software. Due to their dynamic nature, these assets are more likely to develop discrepancies between their actual state and what is recorded in your inventory. For instance, devices that are frequently reissued or replaced should be audited more often to prevent gaps in tracking. Aim to audit high-change assets on a semi-annual or quarterly basis.

Priority 4: Compliance-Regulated Assets

Compliance-regulated assets, such as payment systems, financial records, or health data repositories (e.g., GDPR, HIPAA, or PCI DSS-regulated systems), should be next on your list. These assets need regular review to ensure they meet evolving regulatory requirements. For example, payment processing systems might need to be audited more frequently to confirm compliance with PCI DSS standards. Typically, these assets should be audited semi-annually or as dictated by the specific compliance regulations.

Priority 5: Newly Acquired or Decommissioned Assets

Newly acquired assets, as well as those undergoing decommissioning, should be audited to ensure they are properly recorded, classified, and assigned ownership. It's crucial to confirm that decommissioned assets are securely disposed of or fully retired from

operational use. Audits for newly acquired or decommissioned assets should be scheduled annually or as these changes occur.

Priority 6: Low-Criticality or Stable Assets

Finally, audit low-risk, low-criticality assets that don't experience frequent changes, such as office equipment, peripheral devices, or legacy systems with limited functionality. Since these assets have minimal impact on business operations, they can be audited less frequently. Examples include printers or backup office PCs, which can typically be audited annually.

By following this structured approach, you can audit assets in stages, ensuring that the most critical and dynamic parts of your asset inventory are always up-to-date without overwhelming your teams with unnecessary work on low-risk assets.

Once you've defined the audit scope, the next step is to set clear objectives for each audit cycle. These objectives give purpose to the audit within the established scope and ensure that the audit remains focused and productive.

How to Audit the Asset Inventory?

Regular audits are typically conducted by asset custodians, IT staff, and the information security team. Custodians verify the accuracy of their assets' records, while the information security team ensures that the inventory aligns with compliance and security requirements.

Step 1: Gathering Data

Begin by collecting updated information on your assets, similar to the data collection in the Asset Inventory Mapping Process from Chapter 2. You're verifying and cross-referencing your records, ensuring that no assets have been missed or retired since the last review. Pull data from IT systems, procurement records, and department reports, just as you did during the initial discovery phase.

Step 2: Reviewing Asset Details

This step mirrors the asset classification and criticality assessment from Chapter 3:

Mapping Assets to Business Processes. Revisit your asset classifications - criticality, confidentiality, and lifecycle stage - and ensure they align with current operations. If an asset's role has changed, update its classification to reflect its new importance to the business.

Step 3: Identifying Gaps

Just like the discovery phase described earlier, audits are a chance to uncover new, untracked assets that may have slipped through the cracks - whether it's new software, shadow IT, or hardware. Use this opportunity to identify these gaps and formally add them to your inventory, continuing the process discussed in the Discovering What Already Exists section of Chapter 7.

Step 4: Updating Records

As in Chapter 5: Asset Lifecycle, lifecycle stages, ownership, and custodianship should be updated during the audit to reflect any changes since the last review. This ensures that your asset records stay accurate and relevant, aligning with the asset's current stage and status.

Step 5: Reporting and Follow-Up

Similar to the continuous improvement concept introduced throughout the book, auditing allows you to reinforce accountability. Provide asset owners and custodians with audit reports, including updates on the status of their assets and recommended actions. This callback to the Assigning Ownership and Custodianship section ensures that responsibility for asset security and functionality is maintained as part of your ongoing improvement efforts.

Bringing It All Together: Asset Inventory Management as a Continuous Process

Building an effective asset inventory isn't about reaching a final, perfect state - it's about creating a repeatable, scalable process that continuously supports security, compliance, and risk management.

Throughout this guide, we've covered every step of establishing a strong asset inventory:

- Identifying and Categorising Assets – Ensuring you track what matters most in a structured way.
- Mapping Assets to Business Processes – Connecting assets to the functions they support.
- Assigning Ownership and Custodianship – Making sure every asset has someone accountable for its security.
- Assessing Security Needs and Applying Controls – Implementing protection measures based on risk and business impact.
- Keeping the Inventory Current – Auditing and updating to maintain accuracy over time.

But here's the reality: you're never actually done**.** As your organisation evolves, new assets are added, others become obsolete, and risks shift.

The asset inventory process is an ongoing cycle, not a one-time project.

What Comes Next?

- Revisit your inventory regularly – Identify new assets, remove outdated ones, and ensure categorisation still makes sense.
- Reassess security needs – As threats evolve, controls may need to be adjusted.
- Keep improving processes – The more you refine how assets are tracked, categorised, and protected, the easier ongoing management becomes.

Asset inventory management isn't about perfection - it's about consistency and adaptability. By keeping the process alive and continuously iterating, you ensure that your security strategy stays effective, your organisation remains compliant, and your assets are always protected.

More Resources

This book was brought to you by Kordon.app—the straightforward GRC platform. If you've found value in these pages, you'll likely appreciate our application, which embodies many of the same principles and insights we've explored together. At Kordon, we're dedicated to simplifying information security management and empowering you to build a stronger, clearer, and more effective GRC program.

Links:

- Kordon.app
- ISO 27001 Asset Inventory Example: A Complete List of 140 Assets + Free CSV
- Free Policy Templates – Download Editable GRC Policies