Communications Security Establishment | Centre de la sécurité des télécommunications

# CANADIAN CENTRE FOR CYBER SECURITY

## Using information technology asset management (ITAM) to enhance cyber security


**Management**





Canada

# Foreword

This document is an UNCLASSIFIED publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email, or phone our Contact Centre:

**Contact Centre**
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

# Effective date

This publication takes effect on April 12, 2023.

# Revision history

| Revision | Amendments | Date |
|---|---|---|
| 1 | First release. | April 12, 2023 |
| | | |
| | | |
| | | |

ISBN 978-0-660-48191-3
CAT D97-4/10-004-2023E-PDF

# Overview

This publication provides organizations with advice and guidance related to information technology (IT) asset management (ITAM). It will assist you in gaining a better understanding of ITAM, what it means, why it's important to cyber security, and what your organization should consider to efficiently track, monitor, and maintain your IT assets. Organizations of all sizes can use this guidance to define the set of practices, tailored to their business requirements, that will allow them to track and manage IT assets in their environment.

By implementing an ITAM process, your organization will be able to reduce your IT asset maintenance costs, use licenses more efficiently, increase asset utilization, and better manage security risks. You will be better prepared for compliance audits and increase the efficiency of other information technology infrastructure library (ITIL) processes.

ITAM is an important component to any security risk management framework such as the IT security risk management: A lifecycle approach (ITSG-33) [1], the NIST Cyber Security Framework [2], and the ISO/IEC 27001:2013 [3]. Integrating ITAM into your organization's security framework will help improve your cyber security posture and provide security assurances of confidentiality, integrity, and availability for your business assets.

Organizations who don't have the financial means or human resources needed to implement an in-depth cyber security framework are encouraged to follow our Baseline cyber security controls for small and medium organizations [4]. This publication will help you identify your organization's valuable assets by assessing the injury level associated to them. By doing so, you'll be able to adequately categorize your IT asset, choose the right monitoring and tracking tools, as well as the security controls needed to enhance your cyber security posture.

# Table of contents



# List of figures



# List of annexes

# 1 Introduction

Your organization's business operations have changed considerably when it comes to tracking assets. Organizations have shifted from the use of online spreadsheets to track assets. It's probable that you have too many assets to track manually and require a robust tool to maintain your inventory. Keeping track of all your assets is critical to cyber security and to the operational and financial success of any business and organization.

ITAM is the continuous process of maintaining an updated inventory of all IT assets, both tangible and intangible. It's a set of policies and processes that are used to help organizations account for all assets throughout their lifecycle. ITAM plays a crucial role in the success and growth of any organization. Whether it's managing their IT assets in real time or gaining enhanced visibility, efficient management of IT assets ensures rapid incident detection, response, and resolution which would minimize losses to the organization.

According to the International Association of IT Asset Managers (IAITAM) [5], "IT asset management is a set of business practices that incorporates IT assets across the business units within the organization. It joins the financial, inventory, contractual and risk management responsibilities to manage the overall lifecycle of these assets including tactical and strategic decision making."

A strong ITAM process, will ensure that assets are being deployed, upgraded, and disposed of at the right time and in the appropriate manner. It also allows organizations to quantify risk and ensures that all assets are properly configured and are adequately protected and up to date with security controls and software patches.

# 2 What is an IT asset?

The increasingly complex network of connected devices makes it challenging to identify what counts as an IT asset. Consider an IT asset to be any part of your organization's IT systems for which a compromise, modification, or absence would cause injury or significantly impact your data and software should it be leaked, modified, or rendered inaccessible. Valuable IT assets include data, IT systems, devices, hardware, or other valuable components of your organization's network infrastructure that contains sensitive data or is used to access this data. For example, a desktop computer, laptop, tablet, or mobile phone would be considered an asset, as well as the applications and software running on those devices.

This publication focuses on three categories of IT assets, which we consider to be the top items to inventory and monitor. The three main categories are: software, hardware systems, and critical or sensitive data. The following subsections provide additional considerations for your organization when reviewing assets within these categories.

## 2.1 Software

The software category includes all files and applications run by an organization for work-related purposes. Only approved and secure software should be installed on work devices. Software should be actively monitored to ensure the necessary updates and patches are applied to avoid security vulnerabilities from being exploited by threat actors. In addition to software updates, organizations should also track or monitor the following:

- Applications, software programs, and development tools
- Software licenses
- Cloud-based software subscriptions
- Software as a service (SaaS) subscriptions

ITAM for software would allow organizations to monitor the compliance status of their software licensing agreements, plan for future licensing, and identify the number and types of licenses required to ensure they are getting the best value for each software license usage. Your organization should use automated asset tracking to account for both traditional software and SaaS subscriptions.

## 2.2 Hardware systems

- The hardware category includes all physical devices that comprise an organization's IT infrastructure. When managing these devices at every stage of their lifecycle, organizations will know when it's time to replace or upgrade them or to have them serviced. Hardware systems can be separated into two categories: Infrastructure hardware: All physical components that form the core of an organization's IT infrastructure such as physical servers, storage devices, routers, switches.
- End-user devices: Devices used in the office like desktop computers, keyboards, monitors, printers, and copiers, as well as mobile devices like smartphones, tablets, and laptops.

- Internet of things (IoT) devices: These are objects that can connect to the Internet and collect and exchange information with other devices and systems over the Internet. These “smart” objects include more than the average computer, smartphone, or tablet. They include items like sensors, cameras, microphones, teleconferencing equipment, smart boards, smart speakers, and other voice-activated devices.

## 2.3 Important data

The data category includes sensitive and valuable data that must be considered a key IT asset. This data should consistently be tracked, managed, maintained, and disposed of securely by following the information lifecycle. This lifecycle is similar in nature to the lifecycle followed for hardware or software components of your IT infrastructure. Managing and monitoring sensitive data is just as important as hardware or software tracking, as compromised data can result in costly legal liability to your organization and significant monetary loss. The following actions are recommended to assist you in managing your data assets:

- Maintain an inventory of your stored data
- Document the location of stored data
- Implement access management policies and controls, such as rule-based access control (RBAC), to ensure only those who need to access the data can do so
- Manage the transmission of data using methods such as over-the-air encryption, virtual private network (VPN), and pretty good privacy (PGP) encryption
- Manage the lifecycle of data from when it was initially generated or capture to its eventual archival or deletion at the end of its life

# 3 Why do organizations need an ITAM process?

The main purpose of ITAM is to create and maintain an asset repository that contains an accurate, current, and complete inventory of all the IT assets in your organization. By monitoring your IT assets, you'll have visibility of all assets which will allow you to better understand the following:

- What hardware systems and software exist and what data they contain
- Where these IT components reside in the infrastructure
- How they are used and who is using them
- What they cost to purchase, operate, maintain, and dispose of
- How they are connected to other IT components
- The current phase of their lifecycle
- How they impact IT and business operations

An ITAM program, with the right processes and systems supporting it, can provide your organization with greater scalability, costs savings, optimized asset usage, and better business decision-making processes by allowing your organization to:

- track and maintain IT assets automatically as changes occur in the IT environment
- identify missing IT assets
- document any hardware security issues that could result in increased security risk for the organization
- quantify the cost of underutilized IT assets
- plan for future IT capacity needs
- stay compliant, prepare for audits, and reduce legal and security risks

# 4 Benefits of ITAM to cyber security

An effective ITAM program is an essential part of your organization's cyber security strategy. To be able to protect your IT resources, you should track and manage all components of your IT infrastructure. This will allow you to identify outdated hardware and software and minimize their vulnerability to attacks. ITAM helps maintain the confidentiality, integrity, and availability of information to ensure that this information isn't compromised when critical events arise.

A robust ITAM program will help your organization track and maintain assets as changes occur in your IT environment. Having current and accurate information of all assets will allow your organization to make informed decisions about the available resources and their usage and provides improved overall productivity and utilization of assets.

Here are a few reasons to include ITAM in your **cyber security strategy:**

1. **Mitigates risk:** When an ITAM process is in place you can reduce the threats and security risks that originate from rogue, obsolete, lost, or misconfigured IT assets.
2. **Improves cyber security resiliency and provides a faster incident response:** Allows organizations to focus on securing their most valuable and critical assets by implementing the right security controls. It provides visibility to easily identify the asset affected by an incident and can facilitate root cause analysis. It can also help enable faster incident responses and remediation to security alerts by revealing the location, configuration, and owner of the affected device.
3. **Ensures software is updated and patched:** An ITAM process allows for management of software which can help identify outdated or unpatched software. Older versions of software or unpatched software can be a security risk to your organization.
4. **Determines the role of every software asset:** An ITAM process will allow you to identify all software in use so that you can ensure proper licensing and avoid redundant purchasing. Knowing the operational functionality of each software will allow for proper configuration and reduce security risks.
5. **Provides hardware asset control:** When using ITAM tools you can identify which devices are connected to the network and if they are properly configured and compliant with security controls and current updates. They can also identify obsolete hardware assets and help you to take the necessary steps to minimize the security threats posed by stolen or lost assets.
6. **Identifies the security controls for the IT asset:** When implementing an ITAM process you'll need to identify the IT assets' operational functionalities and what security controls are required to protect them. When an incident occurs, an ITAM process can help provide you with a clear map of the IT networks. This will allow you to identify the points of failure and what needs to be done to fix them and ensure business continuity.
7. **Ensures IT assets categorization:** An ITAM process requires that assets be categorized by their operational functionalities and by the sensitivity of the information they are required to handle. IT assets

that handle sensitive information should be categorized as critical and secured with the right tools, and if compromised, provided with an incident response process to ensure minimal damage to the organization.

## 4.1 Benefits of an ITAM process to the organization's overall operations

1. **Improves visibility and control of their IT infrastructure:** An ITAM process will identify IT components connected to the organization's network, where they reside, how they are used, their current state, and how they impact business operations. It will offer visibility of overused, underused, and obsolete IT assets. Visibility helps organizations improve the performance and efficiency of their assets as well as overhead cost.

2. **Helps identify and track supply chain integrity (SCI) issues:** ITAM offers greater transparency in asset management therefore providing accountability. It improves visibility of the organization's supply chain and supports tracking and assessing SCI issues. Knowing where your assets originated from (manufacturer, supplier, or developer) and when and who performed the maintenance on them can help identify the impact of the SCI issue in the event of an incident. This is especially important when the issue is noticed several years after the initial deployment of the asset. In a similar manner, and along with maintenance records, firmware patches to hardware and versions should also be tracked.

3. **Achieves compliance and better preparedness for audits:** Having an inventory of all assets will undoubtedly help organizations stay compliant and prepare for audits to reduce legal risks. ITAM tools can aid in keeping track of legal, contractual, and regulatory obligations all while improving and reducing cost and reporting time for auditing.

4. **Supports other ITIL practices:** Improves the efficacy of other ITIL practices by providing information about the assets affected by an incident, the problem, or the change in the infrastructure. By knowing the affected assets, organizations can then identify the severity of the incident and its impact by performing a root cause analysis.

5. **Minimizes overall costs:** Reduces cost by ensuring routine inspections and maintenance are performed, thus optimizing existing asset usage. Controls unnecessary IT asset purchases by quantifying the cost of unused hardware and software assets. Tracking assets throughout their lifecycle enables organizations to optimize IT spending by making decisions on operational and future IT capacity needs. ITAM can also improve budgeting and other strategic decision-making processes.

# 5 IT asset lifecycle

All IT assets have a finite period of use and to maximize their usage, your organization should proactively manage and monitor the IT assets at each stage of their lifecycle. This is referred to IT asset lifecycle management (ITALM) and is a core process of ITAM as it helps organizations improve productivity by allowing them to make informed decision on IT needs and services. ITALM will help optimize the efficiency of the asset and reduce unnecessary spending and maintenance costs.

While organizations may have different ways of defining each stage of the asset lifecycle, the generally accepted phases are depicted below in Figure 1.

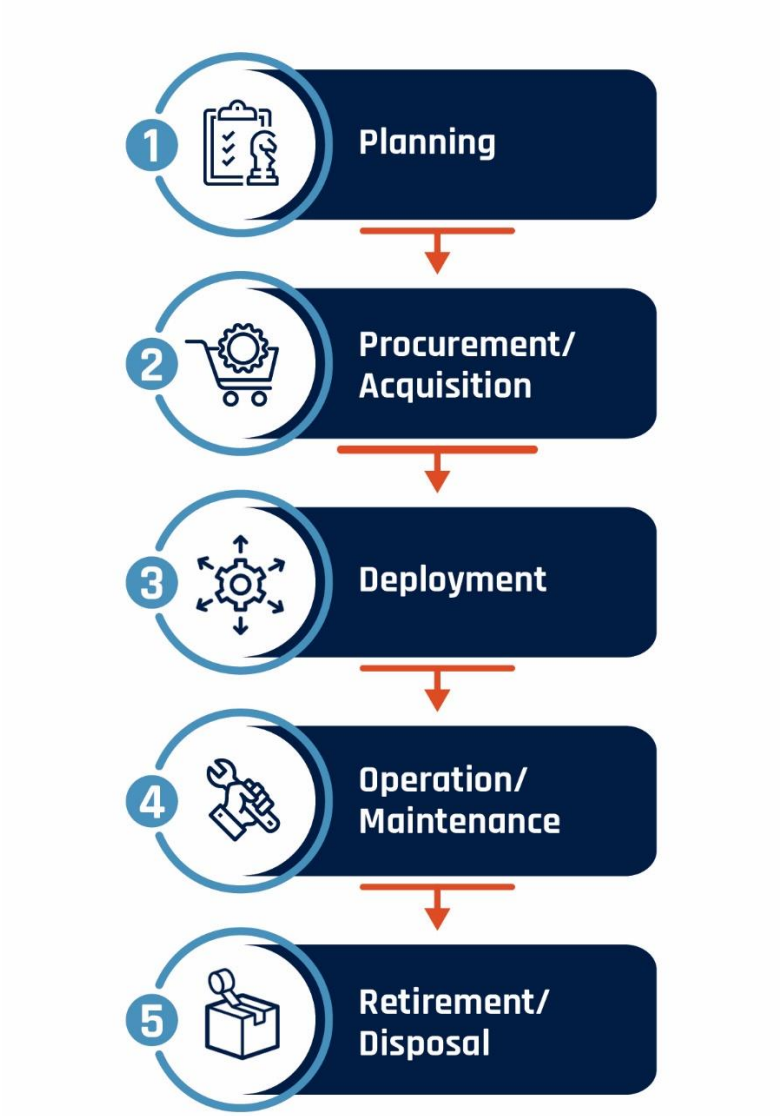


**Figure 1: Asset lifecycle**

Figure 1 caption: The most common phases of an asset's lifecycle are planning, procurement or acquisition, deployment, operation and maintenance, and retirement or disposal.

1. **Planning:** The first phase is the planning, which should ideally occur prior to procuring the asset. Organizations need to identify the business and security needs for the asset with supply chain integrity in mind. They need to justify what it will be used for, how it will be funded, and how it will contribute to the organizational operations based on the evaluation of existing assets and preestablished criteria. An ITAM tool can be used to analyze trends and data and could help identify a future need to procure the asset, preestablishing what value it would add to operations.

2. **Procurement or acquisition:** The second phase is the procurement or acquisition of the asset. This is the cost negotiation phase, where organizations try to identify the most efficient way to meet their goal, budget, and time frame requirements. If the asset is identified as an important and necessary resource, then it's procured, leased, licensed, or built and then installed and/or delivered to the appropriate location. At this point, the asset can then be tracked throughout its entire lifecycle by using an asset management system.

3. **Deployment:** The deployment phase, also known as the usage phase, is the shortest phase of the asset's lifecycle and it's when preliminary inspections are conducted to ensure that the asset is operating successfully and securely. In this phase the asset is introduced to the operators and employees and is integrated into the organization's IT infrastructure where it will interface with other assets to generate increased value.

4. **Operation and maintenance:** The operation and maintenance phase is the most time consuming and often requires the most resources and attention. With the asset now installed and integrated into the IT infrastructure, the asset is improving operations and generating business value. To maximize the value and extend the asset's life, routine maintenance, ongoing monitoring, repairs, upgrades, and updates will be required. Adjustments to the asset will need to be made to keep up with operational and security requirements, maximize investments, and deliver ongoing value.

5. **Retirement or disposal**: When an asset is no longer useful or profitable for the organization and is no longer operating efficiently, or the operational and maintenance costs become too high, it moves into the final phase, the retirement or disposal phase. At this stage the asset must be deactivated, sold, or disposed of in a secure and environmentally safe manner. However, if there is still an operational need for the asset, a replacement is planned for and the assets lifecycle can begin again.

At the end of the asset's life, organizations need to follow environmental regulations and perform secure and sustainable disposal of the asset. Assets that contain sensitive information will need to be sanitized prior to their disposal, by wiping all data and in some cases destroying the media that contains the data, as described in our guidance on IT media sanitization (ITSP.40.006) [6] and the Government of Canada's (GC) Directive on the Management of Materiel [7].

# 6 ITAM best practices

ITAM is an ongoing process and not a one-time project. It should be integrated into your organization's business practices and regularly maintained. Your organization can begin your ITAM implementation and maintenance process by doing the following tasks:

1. Identifying the resources that they need to develop their ITAM process
2. Outlining the capabilities needed to create an ITAM process that will meet their business needs, goals, and budget.
3. Creating a team with designated responsibilities to manage the ITAM process
4. Identifying who is responsible for the different ITAM functions, such as:
    - identifying and categorizing the assets
    - tracking the software licenses
    - identifying and responding to risks
    - monitoring and reporting

Here are some best practices that your organization should follow when developing your ITAM process. Some of these activities can be mapped to the security controls found in ITSG-33 IT security risk management: A lifecycle approach [1]. In parentheses, we will indicate the security controls that are relevant to the activity in question. See Annex A of this document for more information on the controls listed below.

1. Create a comprehensive inventory record

    **(CM-8 Information system component inventory)**

    After developing your ITAM plan, the next step is to create an accurate inventory record. This should include hardware and software IT assets, data, and licenses. A comprehensive record of all assets will ensure that your organization knows what assets you have, where they are located, and who is responsible for them. This can also help avoid duplicate purchases and helps to indicate potential legal and security liabilities.

2. Update the asset inventory regularly

    **(CM-8 Information system component inventory with control enhancement 1)**

    This activity is key to ensure that all assets are appropriately accounted for. Also, this can identify when assets are depreciating and can help budget for future maintenance and replacement costs. Any new asset that is integrated into the organization's infrastructure should be immediately added to the inventory.

3. **Categorize assets**

   **(RA-2 Security categorizations)**

   Categorizing assets and identify the most critical ones is important as this will help organization allocate the required resources to ensure that they are properly managed and secured.

4. **Follow a lifecycle management approach**

   **(PE-20 Asset monitoring and tracking)**

   One of the most critical aspects of IT asset management is understanding the lifecycle of the assets. Every asset has a different lifespan and tracking each asset throughout its entire lifecycle is important. This can help determine when the asset becomes outdated and needs to be replaced or upgraded.

   A designated IT administrator should use an inventory management process that monitors and documents every IT asset's lifecycle status. This process will identify if an asset is in use, in storage, checked out, available or retired. It will allow for close monitoring and will enhance the cyber security of an organization as outdated or obsolete assets create vulnerabilities that threat actors can exploit.

5. **Automate ITAM**

   **(CM-8 Information system component inventory with control enhancements 2 and 3 and MA-6 Timely maintenance with control enhancement 3)**

   Automation can help improve your organization's ITAM practices, increase productivity and reduce risk of human error. Your organizations should use tools to replace technicians who are conducting repetitive and redundant tasks. For example, there are software programs that can automate the asset tracking process. These programs will ensure that assets are being tracked correctly and continuously so that nothing falls through the cracks.

   Automation can also be used for periodic scheduled scans and automatic alerts. These automated checks can help identify assets needing maintenance or upgrading and will alert the technician to fix the issues.

6. **Keep track of software licenses**

   **(CM-8 Information system component inventory)**

   Proper handling and documentation of software licenses is a key aspect of ITAM. A software license also known as a certificate is essentially a contract between the purchaser and the seller. It defines the installation rights, warranties, and stipulates the liabilities. Organizations should know what software they are allowed to deploy, when they expire and need to be either renewed, updated, or cancelled. Knowing this is critically important and will allow organizations to be well prepared for software audits.

7. **Keep records of all maintenance that is performed on the asset**

   **(MA-2 Controlled maintenance with control enhancement 2)**

   Tracking the maintenance that was performed on the asset throughout its lifecycle is useful for identifying SCI issues originating from maintenance providers.

8. **Integrate ITAM with other IT activities within your organization**

   IT asset management is just one part of the larger cyber security strategy and must be integrated into the organization's IT activities, such as IT service management (ITSM) and IT Risk Management. The IT Infrastructure Library (ITIL) framework, for example, incorporates ITAM processes to achieve these goals.

9. **Continuously audit and improve your ITAM policies and process**

   **(AU-6 Audit review, analysis, and reporting and AU-7 Audit reduction and report generation)**

   IT asset management isn't a one-time project. It's a continuous process that involves auditing and improving practices whenever and wherever necessary. Annual audits of IT assets can help track what needs to be updated or replaced. This information allows your organization to make informed decisions about your budget, future purchases, and goals, this also helps to identify areas requiring improvement.

   Your organization can ensure your IT systems remain updated by assessing your assets annually tracking key performance indicators and other relevant metrics and gathering feedback. By doing this, you can facilitate continual improvement and plan for changes, if required, to your ITAM process.

10. **Properly handle old, expired, or obsolete assets**

    **(MP-6 Media sanitization: Control A and B)**

    When an asset is no longer operating efficiently or profitable for an organization and the operational and maintenance costs become too high, it's recommended to upgrade and dispose of the old asset. When disposing of IT assets, organizations must meet regulatory standards. Failure to do can lead to financial penalties, legal repercussions, and damage to the organization's reputation. Assets that held sensitive information at any point of their lifecycle must have their hardware storage media wiped clean of all data prior to their disposal. Within the federal government organizations, there may be a need to wipe and destroy the media, as described in IT media sanitization (ITSP.40.006) [6].

    It's not always possible for organizations to update their assets, and as a result, some will choose to continue to use them even after they become obsolete. Obsolete assets will no longer receive security updates or the newest security mitigations which will increase the impact of vulnerabilities and make exploitation more likely to succeed. If an organization decides to continue to use obsolete assets, we encourage them to follow the National Cyber Security Centre (NCSC) Device Security Guidance [8] and the

Obsolete products (ITSAP.00.095) [9]. They offer advice on how to reduce the risks from using obsolete devices such as smartphones, tablets, laptops, desktop PCs, appliances, or software applications.

# 7 Tools to support ITAM processes

An ITAM tool is a software that is used to manage IT assets throughout their lifecycle from procurement to disposal. It's a centralized system that allows organizations to automatically monitor, track and categorize their IT assets in real time. Asset management software consolidates all critical tasks associated with asset tracking into a single platform that can be accessed through web and mobile applications. ITAM tools can store the following data:

- Inventory information such as asset location, ownership, condition, and lifecycle status
- Contractual information such as licenses, asset warranty, leases, support agreements and other terms and conditions of the contracts
- Financial information that includes purchase prices, costs related to maintenance, repairs, upgrades, and supplier information

When this data is consolidated in one place, it decreases administrative costs, optimizes asset efficiency, and gives your organization greater visibility into asset utilization, costs, and maintenance.

There are many standards and certifications for asset management, including ISO 55001 [10]. Although organizations aren't required to comply to a standard, establishing a standard can help manage the lifecycle of assets more effectively and improve the performance of the assets in an organization.

ISO 55001 is a framework that can help your organization increase control of your daily activities, provide greater return on your assets, mitigate risk, and reduce your overall cost. This standard can be applied to all kinds of organizations with various types of assets. ISO 55001 provides the tools to optimize asset value while ensuring that they meet the necessary safety and performance requirements.

The National Institute of Standards and Technology (NIST) published a cyber security guide for ITAM. The publication was co-written with the National Cyber Security Centre of Excellence (NCCoE) and provides insight on what an asset management system should provide, and how organizations can configure it. This guide is meant to assist organizations when implementing a ITAM solution. It's a proof-of-concept solution demonstrating commercially available technologies that can be implemented to track the location and configuration of networked devices and software across an enterprise. For more information on this publication consult the NIST special publication1800-5: IT Asset Management [11].

## 7.1 Benefits of using ITAM tools

In addition to what was previously mentioned, ITAM tools can provide the following benefits:

1. **Real-time tracking of the asset's activities and condition:**

   ITAM tools can automatically track and record different asset activities such as hours of use, location, modifications and changes made to the asset and more. These actions are continuously monitored and updated to a database in real time. Using automated asset tools such as tracking devices and software is a more efficient and accessible way to manage and allow for quick response to asset issues or misuse.

The majority of asset tracking software offer full reporting functionalities that can be generated upon request.

2. **Removes human error and increases accuracy:**

   With automated asset management tools organizations can collect and store impartial, accurate and organized analytics free from human error. Human error can often go undetected for a prolonged period and trying to identify the source of the error can be nearly impossible. Automation provides a more efficient inventory and better control and precision of the organization's assets throughout their lifecycle.

3. **Reliable maintenance scheduling and early problem detection:**

   Automated asset management tools offer preventative maintenance. They keep track of the asset's condition, installation, and warranty information, as well as maintenance history (who, where and when maintenance was performed). Knowing the maintenance history will also improve accountability. Asset management tools can be configured to automatically send notifications when maintenance is required. This can increase longevity of the asset and identity problems and inefficiencies early to avoid expensive maintenance costs.

4. **Saves time and money:**

   Regardless of the organization's size, performing the asset inventory manually could be a time-intensive task and could require many employees' efforts. An automated asset tracking system could increase efficiency, save time, and cost. Automating asset tracking ensures that the information provided in the asset management database is reliable and current and this could help save cost by preventing unnecessary or repetitive purchases.

5. **Improves and facilitates auditing:**

   Automated asset tracking software provides detailed information about the assets in the organization. It creates a register of information that is needed for auditing purposes such as asset's location, condition, maintenance information, ownership, and more. Accurate audit reports can be easily and automatically generated and will help ensure that organizations remain compliant and always meet all legal standards.

It's important to note, however, that despite all the benefits, automated asset discovery isn't without concern as some assets may not react well to being scanned by these tools. This may need to be taken into consideration, especially in industrial control systems (ICS) or critical infrastructure where reliability or availability is of primary concern. These systems will require a different strategy and/or methodologies to inventory. More on this topic will be discussed in section 7.3.

## 7.2 Criteria to consider when choosing ITAM tools

The ITAM tool should have the capabilities and features needed to support your organization's IT asset-related processes. When reviewing ITAM tools, ensure you evaluate them with the following criteria and functionalities in mind:

1. **Ease-of-use:** User-friendliness is probably the most important criterion in choosing an asset management software. The software should be easy to navigate through and customizable to the organization's unique requirements and needs. The tool should have an intuitive interface that users can easily learn and explore.
2. **Automated asset discovery:** All assets that are connected to your IT infrastructure should be automatically discovered and added to the IT asset inventory. Once installed, an IT asset discovery application communicates with the network's devices to gather hardware and software-related information. It can be configured to periodically flag and remove redundant software assets assigned to previous employees who had privileged access to your network and to unauthorized hardware, software, and firmware components within the IT infrastructure.
3. **Hardware and software metrics tracking:** This includes asset usage rate, monitoring costs, warranty, contract and license status, compliance management, and generation of reports, insights, and alerts.
4. **Integration and compatibility with other systems:** Ensure that the ITAM software can sync well with software that is already in use and integrates seamlessly with your IT infrastructure.
5. **Real-time information:** ITAM software should provide information about IT assets in the present, as changes are noticed. It should provide immediate notifications if it detects a metric beyond the preconfigured threshold setting.
6. **End-to-end lifecycle management:** Each IT asset goes through a lifecycle, starting from the requisition and ending at retirement. ITAM software will track your organization's assets through each stage of their lifecycle and help manage each asset from start to finish. Following the IT assets through their entire lifespan can ensure that you gain maximum value of the assets in your IT environment.
7. **After sales support:** Ensure that you have access to support from the ITAM software provider even after you've purchased their software. Look for a reputable company that offers a support team that is easily accessible and provides prompt assistance.
8. **Configuration and customization:** Select a tool that can be modified to support the requirements of your organizations.
9. **Scalability:** It's important that the software you choose is scalable. Find out how flexible the software and the vendor are in modifying their product to accommodate your organization's current needs and future business requirements.

## 7.3 Additional criteria to consider for OT/ICS systems

Legacy industrial control systems (ICS) network systems are often sensitive to increased traffic or interference from scanning technologies such as discovery tools. The use of scanning technologies on ICS poses risks to your organization, as they may cause unintentional interruptions to the process. The decentralized nature of an ICS network, as well as the minimal capability of the legacy networking equipment, make the use of standard scanning technologies challenging.

When choosing asset discovery tools to integrate into an ICS and operational technologies (OT) infrastructure, operators must be aware of how these tools interact with devices in the OT and ICS network. Incompatible tools can cause disruptions to the infrastructure by triggering certain devices to behave erratically. Some might stop working, restart, or need manual intervention to revert to an operational state. The following list provides some considerations for operators when selecting technologies for asset tracking of OT and ICS systems:

- Ensure the technology is ICS capable, for example, it maintains profiles for data communications protocols
- Use technologies built for ICS networks with integration compatibility with ICS protocols and communications, such as deep packet inspection capabilities
- Use technologies that don't collect, store, or share unauthorized sensitive data
- Ensure the responsible OT/ICS engineer has approved the use of the tool for the specific OT/ICS system

# 8 Network mapping for asset management

An important part of an ITAM process is network mapping. Network mapping is a continuous process of discovering all entities linked to a network to enable granular visibility into your organization's IT infrastructure.

Network mapping tools can create a visual map of your network architecture by automatically discovering network components and topology. These tools can generate key performance insights such as device status, physical connections, and traffic metrics. They also provide real-time automatic visualization of the connections between the network and devices and determine how different endpoints, servers, and networking equipment communicate together. This can help IT teams within your organization detect problems and efficiently troubleshoot issues faster to minimize downtime. In addition to the already mentioned benefits, network mapping can help:

- find and fix single points of failure in the network
- make network analysis, monitoring, discovery, and diagnosis faster and easier
- understand the relationship between the different network components and connected devices
- identify the location of the problematic devices on the network
- detect suspicious connections in the network
- collect information that enables root cause analysis of network issues

# 9 Cloud-based asset management software

Cloud services technology has allowed organizations to reduce their physical space and save on costly infrastructures by eliminating the need to store their servers and data centres on-site. Similarly, cloud-based asset management allows your organization to store data online and run applications without installing software. Your organization does not need to invest large sums of resources in software to help manage and track assets, as cloud service providers (CSPs) often provide such services as part of your service level agreement (SLA). CSPs can also provide customizable asset tracking and reporting for your organization.

If your organization engages with a CSP, be aware that you're giving them direct control over many aspects of your security and privacy. You should engage with CSPs to build a trusting relationship and ensure security parameters and responsibilities are clearly stated in your SLA. Despite the cloud deployment model, your organization is still accountable for protecting the confidentiality, integrity, and availability of the IT services and information hosted by the CSP. Organizations should identify all business and security requirements relevant to ITAM and ensure that security risks are properly managed, cloud-specific security considerations are addressed, and security controls of cloud-based services are properly assessed by the CSP. The CSP should have a comprehensive data security and data privacy policy. They should be compliant with applicable laws and acts in many jurisdictions such as the Privacy Act and Personal Information Protection and Electronic Documents Act (PIPEDA) [12] which governs the collection, use, and disclosure of personal information.

For Government of Canada (GC) departments who are interested in obtaining more information on what to consider when procuring a public cloud service consult the Cloud service provider information technology security assessment process (ITSM.50.100) [13] and Managing the risks to government of Canada data when using cloud services (ITSM.50.109) [14].

## 9.1 Benefits of cloud-based asset management

A cloud-based asset management software system can offer your organization accurate tracking, efficient operations, financial accountability, and easy reporting. Additionally, a cloud-based approach to asset management can provide you with several other benefits, such as:

- **Data protection:** All data stored in the cloud is encrypted and a cloud management system offers security of data with a dedicated security team that works continuously to eliminate any vulnerabilities.
- **Flexibility:** Some asset management software has features that allow for flexibility and customizability. Cloud-based systems offer flexibility and allow your organization to customize the asset tracking service to meet their unique business needs.
- **Scalability:** As your organization grows, it's not always possible for an ITAM software to accommodate and keep up with your evolving needs. Cloud-based software is scalable and can expand to meet the organizations growing needs.

- **Integrations:** Certain cloud-based software products can be easily integrated into your organization's existing infrastructure to give complete visibility and keeping operations running smoothly.
- **Cost Efficiency:** Reduces your organization's cost of data storage systems and financing physical space to store the servers.
- **Greater visibility:** Increases visibility of the asset inventory and more in-depth information to help your organization manage their assets in the most cost-effective way possible.
- **Automation:** Offers automated tools to manage the discovery of assets and provides real-time, up-to-date inventory information. Automation saves your organization time and removes human error from cloud asset management. Automation can also fix vulnerabilities upon detection, without human intervention.
- **Compliance:** Automatically processes regular reviews of the asset tracking system to ensure that all cloud resources are adequately secured and compliant.

# 10 Summary

This publication demonstrates how an ITAM process can help organizations of all sizes enhance and strengthen their cyber security posture and improve their resiliency to cyber threats. ITAM isn't a one-time project but an ongoing process that needs to be evaluated and modified regularly to meet your evolving business needs. It's one element of the larger cyber security strategy and must be integrated into an organization's ITIL processes and risk management framework.

We present the best practices that should be implemented by all organizations when developing their ITAM process. We also recommend automating the ITAM process wherever possible. Automation can help improve ITAM efficiency, increase productivity, and reduce security risks. Cloud-based asset management is also an option for organizations who don't have the physical space or resources to store or operate their own servers and data centres.

By creating an accurate inventory of all IT assets, your organization can gain greater visibility into all aspects of cyber security and compliance. An ITAM process can help you quantify risk and identify what needs protection. It allows for a rapid and thorough response to a cyber incident with minimal impact.

# 11 Supporting content

## 11.1 List of Abbreviations

| Term | Definition |
|---|---|
| CSP | Cloud service provider |
| GC | Government of Canada |
| IAITAM | International Association of IT Asset Managers |
| ICS | Industrial control system |
| IoT | Internet of things |
| ISO | International Organization for Standardization |
| IT | Information technology |
| ITALM | IT asset lifecycle management |
| ITIL | Information technology infrastructure library |
| ITSM | IT service management |
| NCCoE | National Cyber Security Centre of Excellence |
| NIST | National Institute of Standards and Technology |
| OT | Operational technologies |
| PGP | Pretty good privacy |
| RBAC | Rule-based access control |
| SLA | Service level agreement |
| VPN | Virtual private network |

## 11.2 Glossary

| Term | Definition |
|---|---|
| Availability | The ability for the right people to access the right information or systems when needed. Availability is applied to information assets, software, and hardware (infrastructure and its components). Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise. |
| Compromise | The intentional or unintentional disclosure of information, which adversely impacts its confidentiality, integrity, or availability. |
| Confidentiality | The ability to protect sensitive information from being accessed by unauthorized people. |
| Cloud computing | The use of remote servers hosted on the Internet. Cloud computing allows users to access a shared pool of computing resources (such as networks, servers, applications, or services) on demand and from anywhere. Users access these resources via a computer network instead of storing and maintaining all resources on their local computer. |
| Critical infrastructure | Processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across |

| Term | Definition |
|---|---|
| | provinces, territories, and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence. |
| Cyber attack | The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device. |
| Cyber security | The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability. |
| Encryption | Converting information from one form to another to hide its content and prevent unauthorized access. |
| Integrity | The ability to protect information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel. |
| Internet of Things | The network of everyday web-enabled devices that are capable of connecting and exchanging information between each other. |
| IT asset | The components of an information system, including business applications, data, hardware, and software. |
| Security control | A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied by using a variety of security solutions that can include security products, security policies, security practices, and security procedures. |
| Sensitive information | Information that requires protection against unauthorized disclosure. |
| Threat | Any potential event or act (deliberate or accidental) or natural hazard that could compromise IT assets and information. |
| Vulnerability | A flaw or weakness in the design or implementation of an information system or its environment that could be exploited by a threat actor to adversely affect an organization's assets or operations. |

## 11.3 References


| Number | Reference |
|---|---|
| 1 | Canadian Centre for Cyber Security. ITSG-33 IT security risk management: A lifecycle approach. December 2014. |
| 2 | National Institute of Standards and Technology. NIST Cybersecurity Framework. April 2018 |
| 3 | International Organization for Standardization. Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013. October 2013 |
| 4 | Canadian Centre for Cyber Security. Baseline cyber security controls for small and medium organizations. February 2020. |

| Number | Reference |
|---|---|
| 5 | International Association of IT Asset Managers. What is IT Asset Management (ITAM)? |
| 6 | Canadian Centre for Cyber Security. ITSP.40.006: IT media sanitization. July 2017 |
| 7 | Treasury Board of Canada Secretariat. Directive on the Management of Materiel. May 2021. |
| 8 | National Cyber Security Centre. Device Security Guidance. June 2021. |
| 9 | Canadian Centre for Cyber Security. Obsolete products (ITSAP.00.095). March 2023. |
| 10 | International Organization for Standardization. ISO 55001:2014 is the International Standard for Asset Management. July 2014. |
| 11 | National Institute of Standards and Technology. NIST special publication1800-5: IT Asset Management. September 2018. |
| 12 | Office of the Privacy Commissioner of Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA) |
| 13 | Canadian Centre for Cyber Security. ITSM.50.100: Cloud service provider information technology security assessment process. October 2018. |
| 14 | Canadian Centre for Cyber Security. ITSM.50.109: Managing the risks to Government of Canada data when using cloud services. August 2022. |

# Annex A ITSG-33 security control catalogue

## A.1 Operational security control: Configuration management (CM)

Table 1 describes controls **CM-8 Information system component inventory** as defined in Annex 3A of ITSG-33 [1].

**Table 1: ITSG-33 Operational security control: CM-8**

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| CM-8 | Information system component inventory | (A) The organization develops and documents an inventory of information system components that accurately reflects the current information system.<br>(B) The organization develops and documents an inventory of information system components that includes all components within the authorization boundary of the information system.<br>(C) The organization develops and documents an inventory of information system components that is at the level of granularity deemed | **Updates during installations/removals:**<br>The organization updates the inventory of information system components as an integral part of component installations, removals, and information system update.<br>**Automated maintenance:**<br>The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and<br>readily available inventory of information system components.<br>Related control: SI-7.<br>**Automated unauthorized component detection:**<br>(a) The organization employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and<br>(b) The organization takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].<br>Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5<br>**Accountability information:** | CM-2<br>CM-6 |

| | | | | |
|---|---|---|---|---|
| | | necessary for tracking and reporting.<br>(D) The organization develops and documents an inventory of information system components that includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability].<br>(E) The organization reviews and updates the information system component inventory [Assignment: organization-defined frequency]. | The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.<br>**No duplicate accounting of components:**<br>The organization verifies that all components within the authorization boundary of the information system aren't duplicated in other information system component inventories.<br>**Assessed configuration/approved deviation:**<br>The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.<br>Related controls: CM-2, CM-6<br>**Centralized repository:**<br>The organization provides a centralized repository for the inventory of information system components.<br>**Automated location tracking:**<br>The organization employs automated mechanisms to support tracking of information system components by geographic location.<br>**Assignments of components to systems:**<br>(a) The organization assigns [Assignment: organization-defined acquired information system components] to an information system; and<br>(b) The organization receives an acknowledgement from the information system owner of this assignment.<br>Related control: SA-4 | |

## A.2 Operational security control: Physical and environmental protection (PE)

Table 2 describes controls **PE-20 Asset monitoring and tracking** as defined in Annex 3A of ITSG-33 [1].

**Table 2: ITSG-33 Operational security control: PE20**

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| PE-20 | Asset monitoring and tracking | (A) The organization employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].<br>(B) The organization ensures that asset location technologies are employed in accordance with applicable GC legislation and TBS policies, directives, and standards. | None | CM-8 |

## A.3 Operational security control: Maintenance (MA)

Table 3 describes controls **MA-2 Controlled maintenance** and **MA-6 Timely maintenance** as defined in Annex 3A of ITSG-33 [1].

**Table 3: ITSG-33 Operational security control: PE20**

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| MA-2 | Controlled maintenance | (A) The organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements.<br>(B) The organization approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.<br>(C) The organization requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs.<br>(D) The organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs.<br>(E) The organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. | **Automated maintenance activities:**<br>(a) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and<br>(b) The organization produces up-to-date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.<br>Related controls: CA-7, MA-3. | CM-3<br>CM-4<br>MA-4<br>MP-6<br>PE-16<br>SA-12<br>SI-2 |

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| | | (F) The organization includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records. | | |
| MA-6 | Timely maintenance | (A) The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure. | **Preventative maintenance:**<br>The organization performs preventive maintenance on [Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals].<br>**Predictive maintenance:**<br>The organization performs predictive maintenance on [Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals].<br>**Automated support for predictive maintenance:**<br>The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system. | CM-8<br>CP-2<br>CP-7<br>SA-14<br>SA-15 |

# A.4 Management security control: Risk assessment (RA)

Table 4 describes controls **RA-2 Security categorization** as defined in Annex 3A of ITSG-33 [1].

**Table 4: ITSG-33 Management security control: RA-2**

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| RA-2 | Security categorization | (A) The organization categorizes information and the information system in accordance with applicable GC legislation and TBS.<br>(B) The organization documents the security categorization results (including supporting rationale) in the security plan for the information system.<br>(C) The organization ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official's designated representative. | None | CM-8<br>MP-4<br>RA-3<br>SC-7. |

## A.5 Technical security control: Audit and accountability (AU)

Table 5 describes controls **AU-6 Audit review, analysis, and reporting and AU-7 Audit reduction and report generation** as defined in Annex 3A of ITSG-33 [1].

**Table 5: ITSG-33 Technical security control: AU-6 and AU-7**

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| AU-6 | Audit review, analysis, and reporting | (A) The organization reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity].<br>(B) The organization reports findings to [Assignment: organization-defined personnel or roles] | **Process integration**:<br>The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.<br>Related control: AU-12<br>**Correlate audit repositories:**<br>The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.<br>Related controls: AU-12, IR-4<br>**Central review and analysis:**<br>The information system provides the capability to centrally review and analyze audit records from multiple components within the system.<br>Related controls: AU-2, AU-12<br>**Integration/scanning and monitoring capabilities:**<br>The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.<br>Related controls: AU-12, IR-4, RA-5<br>**Permitted actions:** | AC-2<br>AC-3<br>AC-6<br>AC-17<br>AT-3<br>AU-7<br>AU-16<br>CA-7<br>CM-5<br>CM-10<br>CM-11<br>IA-3<br>IA-5<br>IR-5<br>IR-6<br>MA-4<br>MP-4<br>PE-3<br>PE-6<br>PE-14<br>PE-16 |

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| | | | The organization specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information.<br>**Full text analysis or privilege commands:**<br>The organization performs a full-text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis.<br>Related controls: AU-3, AU-9, AU-11, AU-1<br>**Correlation with information from nontechnical sources:**<br>The organization correlates information from nontechnical sources with audit information to enhance organization-wide situational awareness.<br>Related control: AT-2<br>**Audit-level adjustment:**<br>The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information. | RA-5<br>SC-7<br>SC-18<br>SC-19<br>SI-3<br>SI-4<br>SI-7 |

| Number | Control | Requirement | Control Enhancements | Related ITSG-33 Controls |
|---|---|---|---|---|
| AU-7 | Audit reduction and report generation | (A) The information system provides an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents.<br>(B) The information system provides an audit reduction and report generation capability that does not alter the original content or time ordering of audit records. | **Automatic processing:**<br>The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].<br>Related controls: AU-2, AU-12<br>**Automatic sort and search**<br>The information system provides the capability to sort and search audit records for events of interest based on the content of [Assignment: organization-defined audit fields within audit records]. | AU-6 |