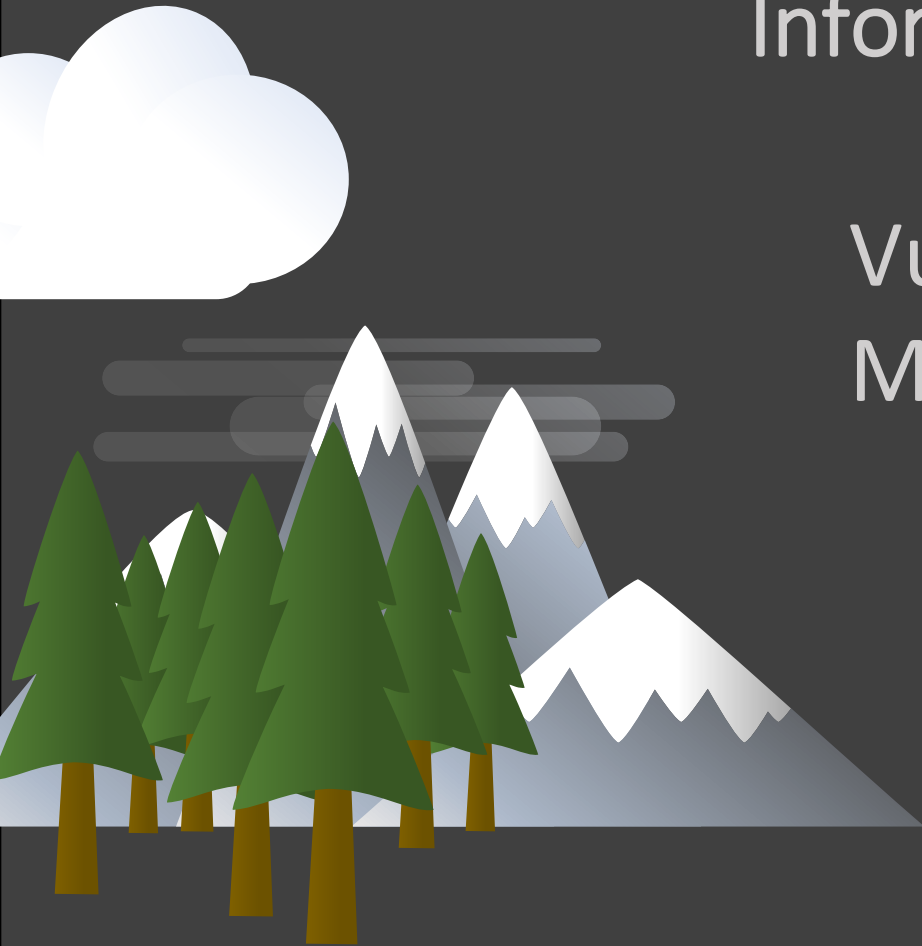




OCIO

Information Security Branch

Vulnerability and Risk Management Training

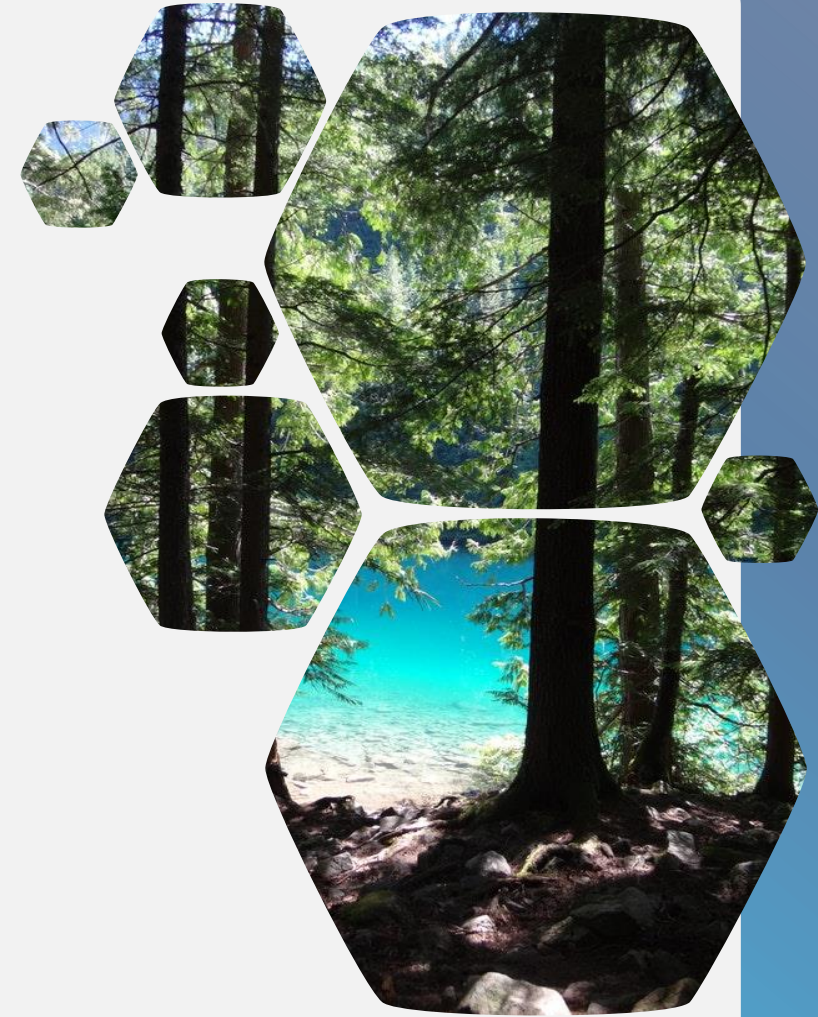


Secure IT Asset Management

Information Security Branch



Office of the Chief
Information Officer



Welcome to a B.C. Provincial Government training course from the Information Security Branch

Here are a few **tips** to allow you to make the most of your learning experience:

Course navigation is through the arrow keys on your keyboard or using your mouse to click the icons at the bottom of the screen. Take your time as you work through this course, it may take a couple of readthroughs of the entire course to understand all the concepts and terminology.

If you are unsure of any of the terms used in this course you can look them up in the **Glossary**, which is located at the end of the course.



First Nations Acknowledgment and Respect

This course was created by those working within the communities of Southern Vancouver Island and the South Gulf Islands that are located in the traditional territories of the Lekwungen (Esquimalt and Songhees), Malahat, Pacheedaht, Scia'new, T'Sou-ke and W̱SÁNEĆ (Pauquachin, Tsartlip, Tsawout, Tseycum) and Quw'utsun (Kw'amutsun, Qwum'yiqun', Hwulqwselu, S'amuna', L'uml'umuluts, Hinupsum, Tl'ulpalus) peoples.

We acknowledge and respect our traditional hosts.





Learning Objectives

This training course is just one part of the Office of the Chief Information Officer (OCIO) Information Security Branch (ISB) education series.

The goal of this course series is to inform staff, information security personnel and all other staff, on information security topics. Raising our awareness regarding information security will help to protect all of the B.C. Government from breaches and other issues that could mar government functions, leak residents' data and even erode trust in the ability of the provincial government. Working together we can keep the B.C. Government safe.

If further assistance is needed understanding, accessing or completing this course, please email:

VulnerabilityandRiskManagement@gov.bc.ca

B.C. Provincial Government Information Security Branch

Information security, management and technology play a crucial role in government service delivery. As such, the province takes an approach that **balances** the protection of sensitive information alongside sharing that information within government programs, the broader public sector, and residents.

Through its Information Security program, the Province promotes a **risk based approach** to information security and ensures programs, plans and processes are in place to **appropriately protect** the confidentiality, integrity and availability of Government information. The Province provides subject matter experts (SME) in support of information security awareness, vulnerability and risk management, advisory services, security operations, and investigations and forensics.

For more information on the ISB you can visit our website at:

<http://www.gov.bc.ca/informationsecurity>

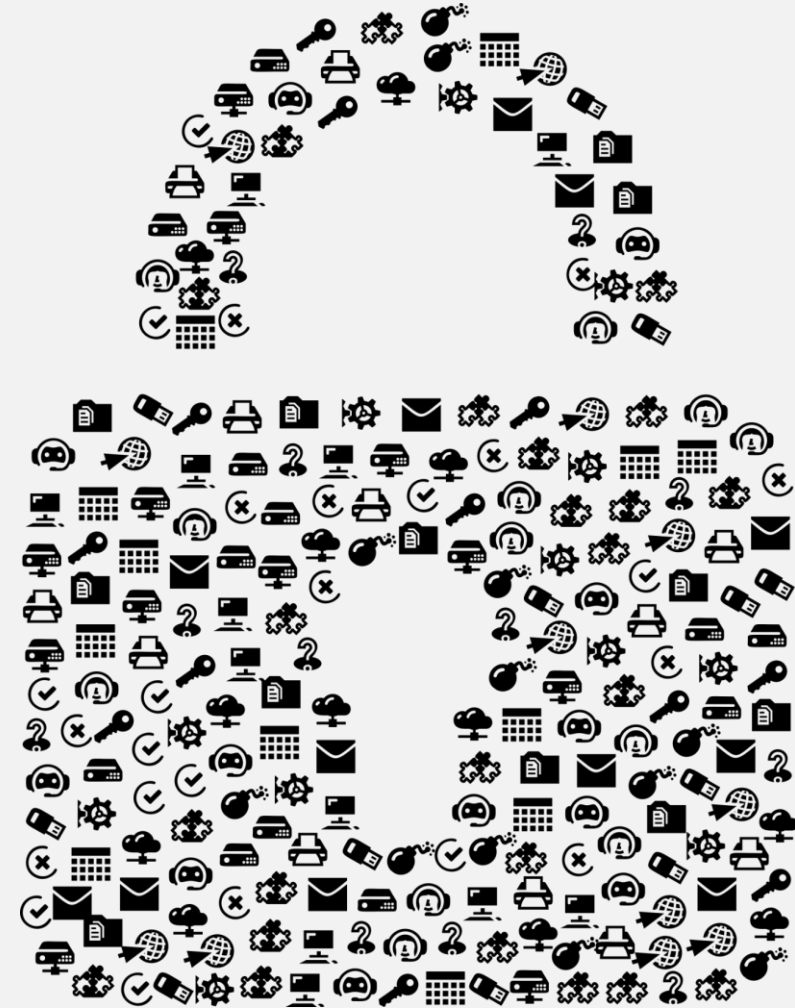


Course Information

This is the OCIO Information Security course on Secure IT Asset Management (SITAM). You may be familiar with asset management but this course approaches the subject from a different perspective, through the lens of information security.

At the beginning the course will provide a background on what SITAM is, followed by the benefits that can be gained by its implementation. Next is information on a framework for using SITAM and some best practices.

Then the course moves into the asset lifecycle and how to create an inventory record, communication and data flows, as well as how to define critical assets. Lastly the course will run through secure IT asset management within the B.C. Government followed by a course summary and glossary.

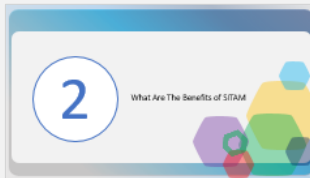


Course Sections



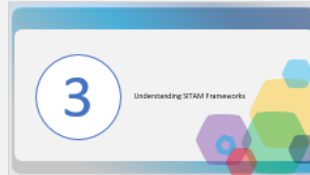
What is IT Asset Management and SITAM

NIST Secure IT Asset Management Framework
Different Asset Types of ITAM



What Are The Benefits of SITAM

Why Asset Management is Vital for Information Security
Six Questions for Asset Owners
SITAM Impact on Business

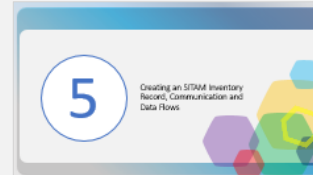


Understanding SITAM Frameworks

Creating a SITAM Framework
ITAM Framework Categories
Ten SITAM Best Practices

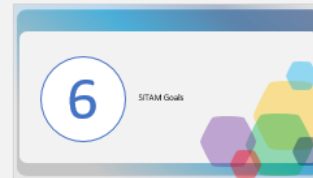


The Asset Management Lifecycle



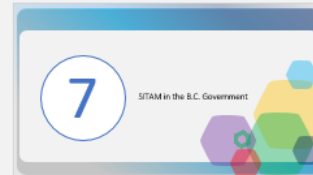
Creating an SITAM Inventory Record, Communication and Data Flows

What is in Scope of Record Inventory?



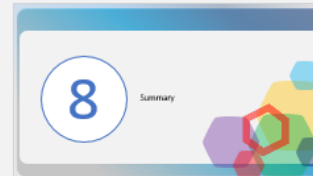
SITAM Goals

Defining Critical Assets



SITAM in the B.C. Government

SITAM Policies and Standards



Summary & Course Glossary






What is IT Asset Management & Secure IT Asset Management



What is IT Asset Management

The International Association of Information Technology Asset Managers¹ (IAITAM) defines IT Asset Management (ITAM) as:



A set of business practices that incorporates IT assets across the business units within the organisation.



ITAM tracks how IT assets are being used and where changes, such as updates or replacements, may be needed. A working ITAM process will save money as it identifies software you might no longer need, are over licensed for, or an IT hardware asset that you are leasing but no longer using.

Business areas keep a close track of financial assets, such as salary and purchases, as well as other assets like buildings, vehicle fleets, and other machinery. Your IT assets are just as valuable when it comes to purchasing, yet even more so as digital assets contain data such as personal information, medical or judicial. Tracking important digital assets is vital to the digital privacy and security of the residents of British Columbia.

1. <https://iaitam.org/>

What is Secure IT Asset Management

The ways we access and protect government's data continue to evolve but the reasons for doing it stay the same; data is at the core of the B.C. Government. To effectively protect it, we need visibility and control over all our assets.

Secure IT asset management (SITAM) is the foundation of risk management. We need to have an informed understanding of our IT environment as it will improve not only our operational ability but our information security too.

SITAM is key to managing the growing volume of devices and systems within government. It also acts as an early warning system; helping to identify risk earlier in the event of a security breach and delivering a quick and effective response.



SITAM is defined by the National Institute of Standards and Technology¹ (NIST) as:

“The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are **identified** and managed consistent with their relative **importance** to organisational objectives and the organisation's **risk strategy**.”

1. <https://www.nist.gov/>

NIST and the Center for Internet Security¹ have developed frameworks to help organisations develop strong information security programs for managing the risks of attacks.

According to these frameworks, **identifying and managing IT assets is the first step in effective information security risk management**. Assets are not possible to protect, monitor, or respond quickly to incidents involving them, if they are not known about.



The NIST **Secure IT Asset Management Framework** is available for free from:
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf> (PDF link).

The NIST 'Cybersecurity IT Asset Management Practice' demonstrates asset management implementations. It shows how it is possible to undertake physical asset tracking, IT asset information, physical security, vulnerability management and maintenance of compliance related information.

1. <https://www.cisecurity.org/>

Different Asset Types of ITAM

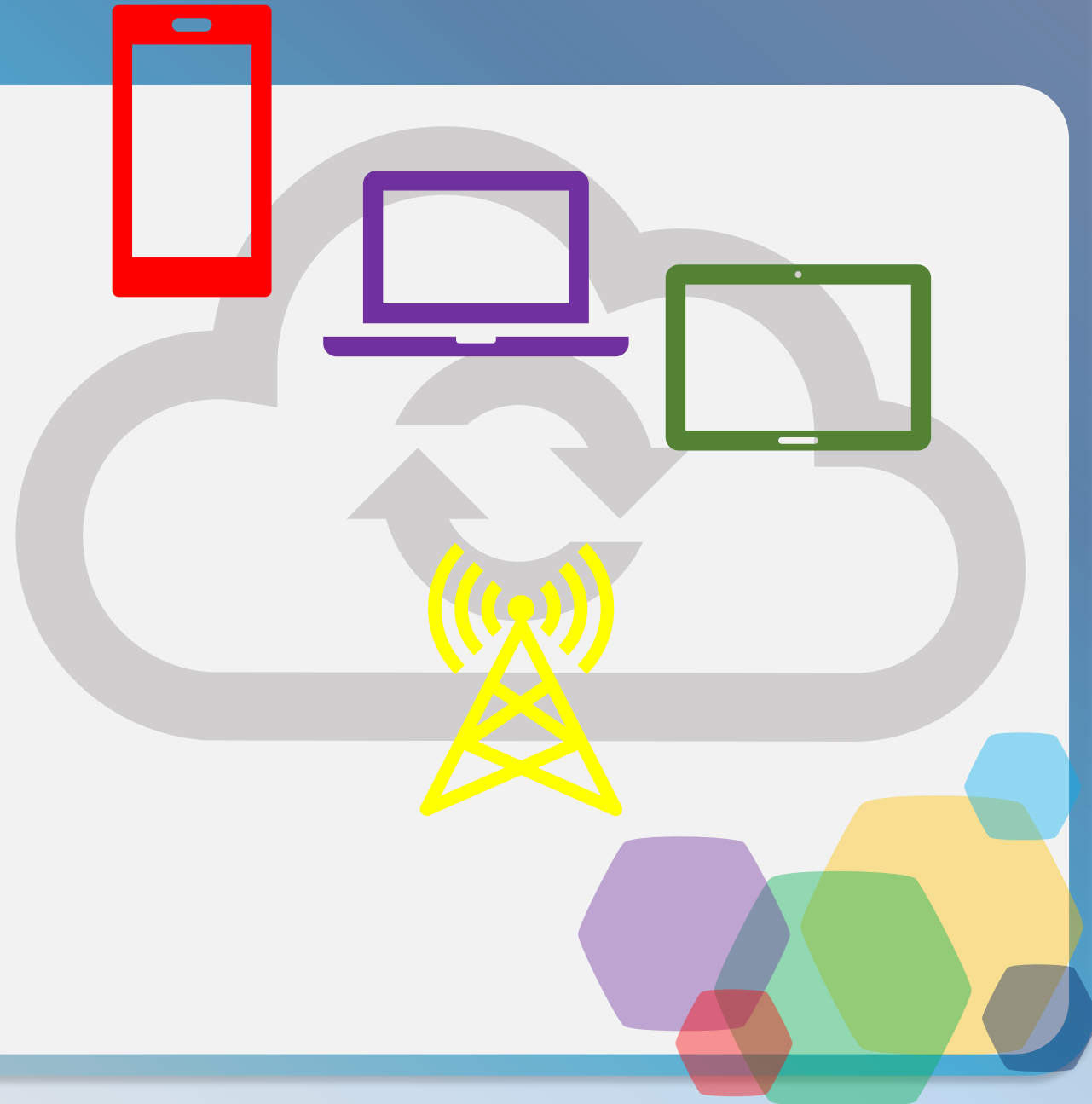
There are many different asset types, and these will vary depending on the business. These different asset types can include, but are not limited to:

Physical: The discovery of hardware. This includes PCs, laptops, printers, copiers, internet of things (IoT) devices, and any other hardware devices used for IT and data. Like smart TVs, smart appliances, lightbulbs, switches, industrial machines, and so on.

Digital: The tracking of information, documents, photos, videos, and other digital data.

Software: Software, compliance, licensing, finding both legitimate, and user installed software (known as shadow IT).

Mobile: These devices are used more and more outside of the office, they are also the most vulnerable to loss, and shadow IT.



2

What Are The Benefits of SITAM



The Benefits of SITAM

SITAM is more than just choosing the best software and devices for use within government, a full SITAM process will provide benefits such as:



1. Better overall data security.
2. Improved data flow awareness.
3. Better communication and understanding between business areas.
4. Improved customer service.
5. Cost reduction of IT assets, both hardware and software, from an ongoing periodic asset review.
6. Improved budgeting and decision-making, due to increased understanding of IT assets, and their role.
7. Less breaches of IT infrastructure by ensuring that software is correctly versioned, patched and updated.
8. Improved business continuity, and disaster recovery.



- 9. Enables faster responses to information security events.
- 10. Improved information security by an increased awareness and focus on the most valuable, or critical, assets.
- 11. Reduced reporting time for both management and auditing.
- 12. Creates lists of software licenses in use, with compliance statistics.
- 13. Reduced help desk response times, as staff already know what is installed and where.

Risk assessment is a vital part of secure asset management. Different business areas should collaborate and share risk assessments. As this will allow for cost, time and effort savings.

This will help government to create faster, and more accurate, SITAM.



Why Asset Management is Vital for Information Security

We can't value what we can't measure, and we can't measure what we don't know about. **Discovery is the key.**

We need to know what we have, where it is, and what it is used for. Then repeat that question periodically so that the inventory can remain up to date.

After understanding what we have, we need to **protect each asset consistent with its importance.**

For example, it is easy to assume that those at the top of an organisation have the most important and critical laptops, but they're actually very few in number, and more likely to be spear-phished¹. Remember, to assess risk, we have to keep in mind **impact and likelihood.**

We have many other staff travelling with mobile devices, to and from work, working on different sites, using cabs, and so on. All the places where devices might go missing with business confidential information, or personal information, our valuable data.

Accurately accounting for devices and software is the first step in effective SITAM.



1. Spear-phishing is a targeted phishing attack, where an email is sent to someone with a goal of tricking them into inadvertently downloading malicious software.

Six Questions for Asset Owners

A successful SITAM program means that asset owners should be able to answer **six essential questions about every asset**:



1. Is the asset or data known, managed and classified?
2. Where is it?
3. What is it?
4. Is it up-to-date? (The core hardware, software, data, and so on).
5. What additional customisation, hardware or software has been made, or is installed?
6. Does it adhere to security policy, and any other ministry specific guidelines?

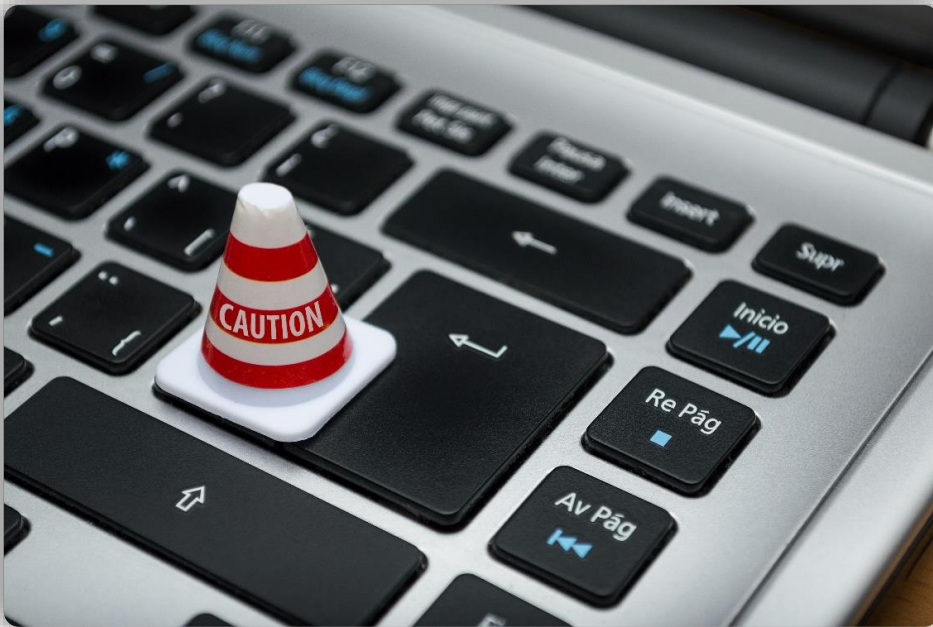
The key to reaching the point where these six questions can be answered is down to good investigation, and communication.



SITAM and Impacts on Business

A HDI study¹ showed that the main reason companies had hardware asset management in place was for *inventory tracking* (96%), not *data security and compliance* (55%). **This is the wrong way around.** Asset management should be a part of your security solution.

It is intangible assets, those that are not physical, are what should really concern us, and it is those we have the most of. What's the cost of losing a physical asset? Perhaps \$2,000 for a laptop. What's the cost of a data breach that happens as a result of a poorly secured lost laptop? On average about \$3.62 million².



The value of our physical business assets is not close to the value of the **data on those assets**.

Physical assets can be replaced, but the data on them might not be so easy to replace. And that doesn't take into account the many ways that the B.C. Government's infrastructure could be exploited by that lost data, or residents potential loss of trust in government.

1. <https://www.thinkhdi.com/~media/HDICorp/Files/Research-Corner/rb-asset-mgmt-may15.pdf> - PDF link
2. <https://www.scrypt.com/blog/average-cost-data-breach-2017-3-62-million/>

Why many enterprises need modern SITAM

- 43% of businesses still track IT assets in spreadsheets.¹
- Businesses, on average, spend 80% of their time reacting to maintenance issues² that arise rather than preventing them. Any business can save 12-18% by investing in preventive instead of reactive maintenance.³
- In an information security incident the most expensive component is information loss, which represents 43% of the overall costs.⁴
- 41% had at least 1,000 sensitive files, and 58% had 100,000 folders, open to all employees.⁵
- On average, 54% of businesses stored data was outdated and no longer useful.⁵

Wasted time with legacy SITAM

- 29% of IT organisations spend excess staff hours trying to reconcile inventory and assets.⁶
- 28% spend excess hours dealing with out-of-warranty and out-of-support policy assets.⁶

Big savings for SITAM adopters

- Businesses that successfully implement SITAM can achieve up to a 30% cost savings in the first year, and at least 5% savings in each of the subsequent five years.⁷

1. <https://www.ivanti.com/blog/how-it-professionals-are-managing-assets>
2. <https://www.capterra.com/resources/the-top-maintenance-statistics-you-should-know-for-2017/>
3. <https://transcendent.ai/blog/asset-management/42-roi-statistics-that-prove-you-need-a-maintenance-management-system/>
4. <https://www.accenture.com/us-en/about/security-index?src=SOMS#block-insights-and-innovation>
5. [https://info.varonis.com/hubfs/2018 Varonis Global Data Risk Report.pdf](https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf)
6. <https://www.ivanti.com/blog/study-it-professionals-assets-spreadsheets>
7. https://www.gartner.com/imagesrv/media-products/pdf/provance/provance_issue1.pdf





Understanding SITAM Frameworks





Creating a SITAM Framework



SITAM is the **first requirement** of risk management.

Asset management should not be about creating a list, in order to be ready for the next audit.

SITAM is key to safely managing devices and systems inside government. It will help to identify potential risks earlier in the event of a security breach, and help deliver a quicker and more effective response to those incidents.

Understanding our assets across their whole lifecycle will improve our overall security posture.

The NIST **Cybersecurity Framework**¹ focuses on using business drivers to guide information security, as part of any organisation's overall risk management.


The NIST framework consists of three parts:

1. The Framework Core
2. The Implementation Tiers
3. The Framework Profiles

“The framework core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the core provide detailed guidance for developing individual organisational profiles.” - NIST

1. <https://www.nist.gov/cyberframework>






The NIST framework helps plan and prioritise activities with its business and mission requirements, risk tolerances, and resources. Its framework provides a method to view, and manage security risks.

SITAM is a subdivision of the overarching NIST cybersecurity framework.

“While a physical asset management system can tell you the location of a computer, it cannot answer questions like, “What operating systems are our laptops running?” and “Which devices are vulnerable to the latest threat?” An effective IT asset management (ITAM) solution can tie together physical and virtual assets and provide management with a complete picture of what, where, and how assets are being used. ITAM enhances visibility for security analysts, which leads to better asset utilization and security.¹ – NIST.”

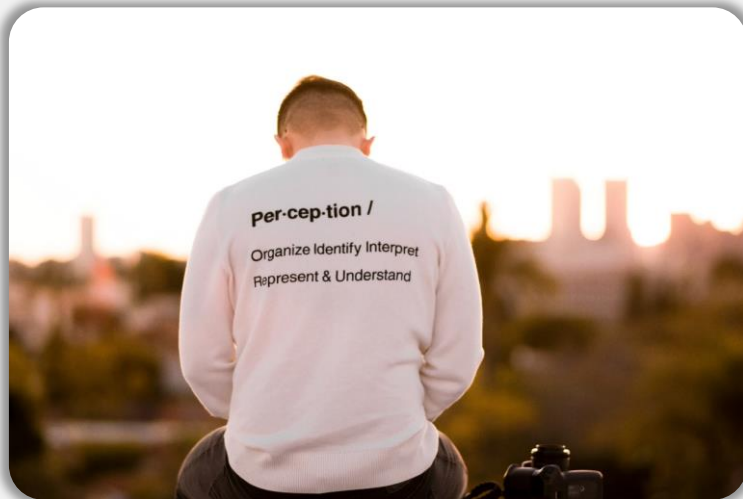
1. <https://www.nccoe.nist.gov/publication/1800-5/VolB/>





Each of the NIST functions are split into categories. These categories group the outcomes associated with those activities. For example, asset control, asset management, and detection processes. Further subcategories divide a category into specific outcomes. For example, catalogs for information systems, notifications from detection systems are reviewed, and data-at-rest is protected.

Here are the six **NIST Framework Functions**¹:



- 1. Identify:** Identifying the key aspects of the business, including systems, data, personnel, policies and procedures, and the environment. At this stage time needs to be taken to understand what possible attacks could be made, and how these risks can be addressed.
- 2. Protect:** The creation of safeguards, and protocols, that limit threat risk exposure. This involves sub categories that include:
 - Access control.
 - Data security.
 - Employee training and awareness.

1. <https://www.nist.gov/cyberframework>



3. **Detect:** This requires a security monitoring infrastructure. It also involves the constant testing, maintenance, and auditing, of these monitoring efforts.
4. **Respond:** Responding to a threat with a planned strategy reduces the threats impact. This includes learning from incidents so that mitigations can be in place against future attacks.
5. **Recover:** Adopting plans that recover, or replace, any lost functionality due to an incident. This would include examples such as:
 - Taking backups.
 - Disaster recovery.
 - Business continuity plans.



Ten SITAM Best Practices

At a high level, both the NIST and CIS cybersecurity frameworks encompass the following **ten best practices of SITAM**:

1. Create an **inventory database**. This identifies, tracks and prioritises devices, systems, and applications.
2. Add assets to **inventories**. This means that assets are monitored, and that business areas and ministries collaborate to ensure they are accurate, complete and current. Assets need to be labelled based on the risk that is posed to them, and the ministry or business area's risk appetite.
3. To create and maintain maps that show **the interconnections between devices, systems and applications**. Key or critical business functions should also have data flows created.
4. Create and document **information security roles, and responsibilities**. These should include third-party stakeholders, and what IT assets are managed by them.





5. Create and manage an **asset management life cycle** strategy, to understand when devices will need maintenance, or replacement.
6. Understand and document device capabilities, use cases, and **how they are actually used within the business**. This will lead to better, and more efficient use of, those assets.
7. Undertake accurate asset **risk assessment and risk management**. Understanding the risks that are involved with an asset allows for the business to mitigate, or accept, that risk.



8. SITAM also involves documenting, and depending on the asset, managing those finite resources.
9. Finding and documenting **ghost assets**. These are assets that have been lost, stolen, or decommissioned, but are undocumented and might still be in the asset records. If asset inventories are not maintained these devices may not be patched, serviced, or replaced.
10. Create an **ongoing asset monitoring** process, both digital and physical. This process will help to ensure that devices are less likely to be lost, or stolen.



Characteristics of an Effective SITAM Solution

As well as those best practises, the NIST framework¹ helps define the characteristics of an effective established SITAM solution. In other words, **these are the goals to aim for:**

1. Complement existing asset management, security, and network systems.
2. Provide application programming interfaces to communicate with other security devices and systems such as firewalls and intrusion detection and identity and access management systems.
3. Know and control which assets, both virtual and physical, are connected to the enterprise network.
4. Automatically detect and alert when unauthorised devices attempt to access the network, also known as asset discovery.
5. Enable administrators to define and control the hardware and software that can be connected to the corporate environment.
6. Enforce software restriction policies relating to what software is allowed to run in the corporate environment.
7. Record and track attributes of assets.
8. Audit and monitor changes in an asset's state and connection.
9. Integrate with log analysis tools to collect and store audited information.



1. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.1800-5.pdf>





The Asset Management Lifecycle

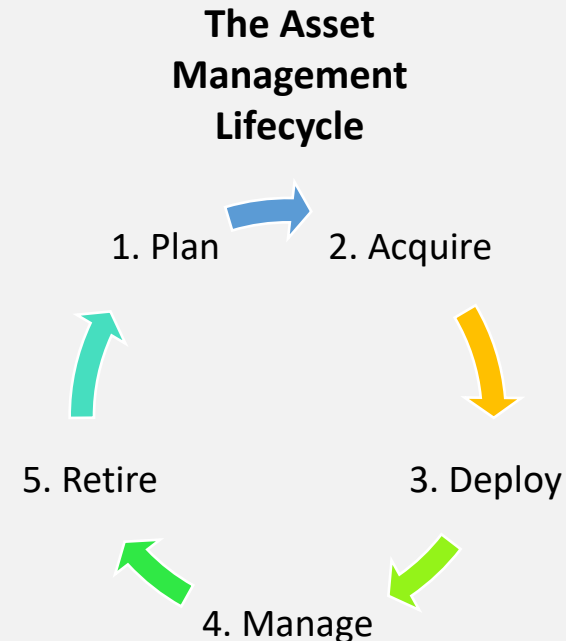


The Asset Management Life Cycle

A key process within SITAM is the understanding of the **asset management life cycle**. An asset lifecycle is a process that helps to define and understand the current environment, and its needs.

Defining an asset's life cycle is a risk management activity that should be used for all assets, both physical and intangible, such as data. Understanding the lifecycle will show when maintenance is needed, or if a device needs to be replaced, new software installed, and so on. Lifecycle management will also create a priority list of devices that need attention, that otherwise might not be updated and lead to a security breach.

Understanding the life cycle starts with knowing where assets are, and what they are used for. It is then possible to estimate costs for the tasks those assets are used for. Understanding the use case, and the costs involved, allows for the creation of more accurate budget planning.



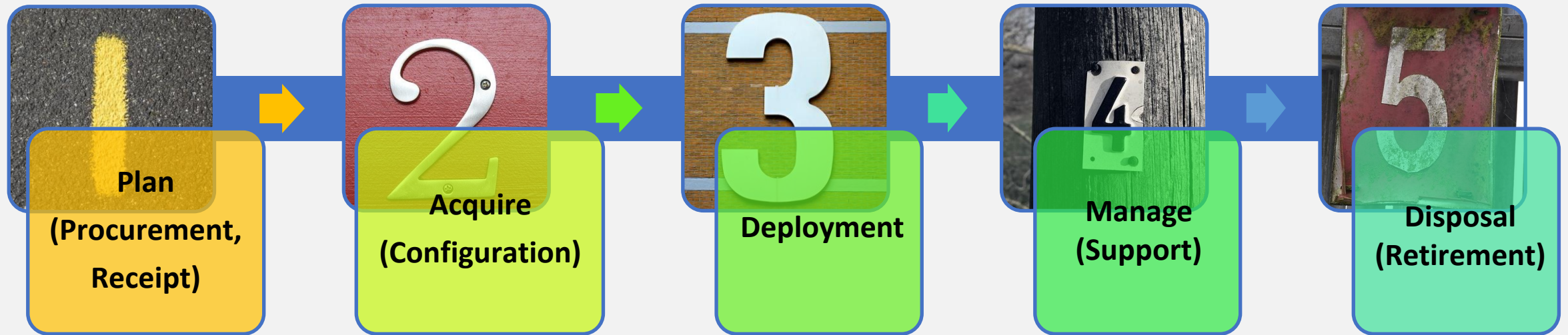
All assets should have a documented lifecycle, one that is ideally collaborated on, or shared with others. This will save time, effort, and money across government. It should be noted where in that lifecycle stage each asset is at.



Lifecycle questions could also include:

1. What software licence, age, renewal, or optimisation needs are needed?
2. Is this audit and compliance ready?
3. Is this cloud enabled?
4. What is the vendor lifecycle, when does the vendor cease publishing patches?
5. Is the dataflow documented?

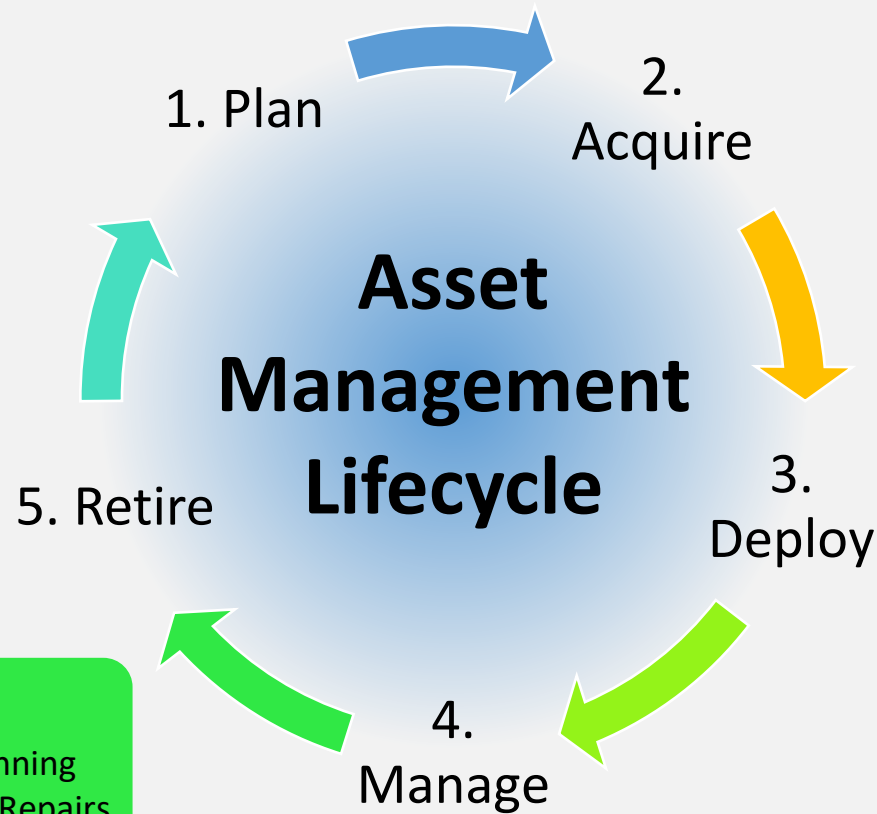
The Asset Lifecycle: High Level



Benefits of a good IT asset life cycle management solution:

1. Forecast your needs better.
2. Make informed purchasing decisions.
3. Be proactive when it comes to replenishing resources.
4. Improve the quality of IT services.
5. Know the total cost of ownership of an asset.





Planning & Purchase

- Asset Procurement Planning
- Asset Vendor Management
- Quotes
- Purchase Order

Disposing & Reconditioning

- Asset Retirement Planning
- Asset Decommissioning
- Reconditioning & Refurbishment
- Re-inspection & Re-admission
- Reports

Maintenance & Compliance

- Regular & Preventive Maintenance Planning
- Asset & Parts Issue for Maintenance & Repairs
- Maintenance Checklist
- Post Maintenance Inspection
- Accident or Failure Registration
- Asset Calibration, Certification, Insurance Plan
- Alerts & Reminders
- Asset Audits
- Maintenance & Asset Health Analysis Reports

Acquisition & Commissioning

- Asset Inward & Inspection
- Asset Returns
- Commissioning & Trail Run
- Asset & Parts Registration

Allocation & Tracking

- Asset Allocation Planning
- Asset Allocation Workflow
- Operator Assignment Planning
- Operator Assignment
- Asset Transfer Planning
- Asset Transfer
- Duty Slips
- Daily Utilisation Logs
- Plan vs Actual Analysis
- Extensive Asset Utilisation Reports

Security

- User ID & Authentication
- User Authorisation
- Role Based Access
- Privilege Audit Trails

Reporting

- Standard Reports
- Graphical Reports
- Man. Info. Sys. (MIS)
- Reports with Drill Downs
- Dashboards & Analytics

General

- Latest Technology
- Completely Browser Based
- Integration with Enterprise Resource Planning (ERP)
- Integration Ready



Creating an SITAM Inventory Record, Communication and Data Flows



Creating an IT Asset Management Inventory Record: The Basics

Assets include the tangible (laptops and printers) and intangible (data, intellectual property, processes, network bandwidth), as well as brand, trust, and public perception.

When creating the asset inventory there are three steps to take:

1. **Filtering of Assets**

- What needs listing and where.

2. **Prioritisation of Assets**

- What is considered important or critical.

3. **Categorisation of Assets**

- Hardware, software, ministry, use case, and so on.

Potential risks should then be mapped to those assets. They can be further categorised as needed by the business, for example:

- **Classification** – Public, business sensitive, confidential
- **Information type** – PII, commercial, medical, judicial and so on
- **Value**, financial or non-financial value

An auditor will expect to see an inventory system that will cover all our relevant assets. Each of our assets must be assigned an owner, and assigned a security classification.



This inventory record content example is based on the [ISO 27001](https://www.isms.online/iso-27001/annex-a-8-asset-management/)¹. ISO requirements state that all **information assets** are to be considered, not just physical assets. This includes anything of value to the business, anywhere information is stored, processed, and accessed. The focus is on the **information**, less so the network or device.

Example IT Asset Management Inventory Record Contents

Asset Types

- Information (or data).
- Data flow.
- Intangibles – such as IP, brand and reputation.
- People – Employees, temporary staff, contractors, volunteers, and so on.

The physical assets associated with their processing and infrastructure:

- **Hardware** – Typically IT servers, network equipment, workstations, mobile devices and so on.
- **Software** – Purchased, or bespoke, software.
- **Services** – The actual service provided to end-users (for example, database systems, e-mail and so on).
- **Locations & Buildings** – Sites, buildings, offices and so on.
- **Communication**, flow and methods.

Logical Groupings

Any type of asset can be grouped together logically, according to a number of factors, such as:

- Data and Information Classification – for example, public, business sensitive, confidential, and so on.
- Information type – for example, PPI, commercial, and so on.
- Financial, or non-financial, value.

1. <https://www.isms.online/iso-27001/annex-a-8-asset-management/>

What is in Scope?

There are many possibilities when it comes to the scope. Various business functions will be itemised, related stakeholders brought in, and potentially other business areas.

To understand the potential scope, a number of different factors must be considered, such as the ministry, business units, departments, service lines, physical locations, mobile workers, geographical distance, system complexity and age.

If considering leaving something out of scope, ask the question - **what would the impact on the business area, or others business areas, and other related stakeholders?** If the impact is severe, then reconsider leaving it out of scope.

The scope should include business areas that need to create, access or process, any data that is considered critical. Lastly, also look at what is in your control, and what you cannot control.

Understanding your scope might not take very long, or it might take weeks, or longer. A complex project that spans multiple ministries or business areas might take a long time to scope correctly.



Creating a Map of Key Organisational Communications and Data Flows

We need to have guidelines and procedures that ensure our communication, and data flows, are mapped out, continuously updated, and include our critical information assets.

Firstly, look at the communication flow for a specific asset. Although it could be very complex, most often it is a short data, or communication flow, that lists the roles and types of information of that asset, and how that communication occurs.



The Who, How, and What

This simple maxim covers:

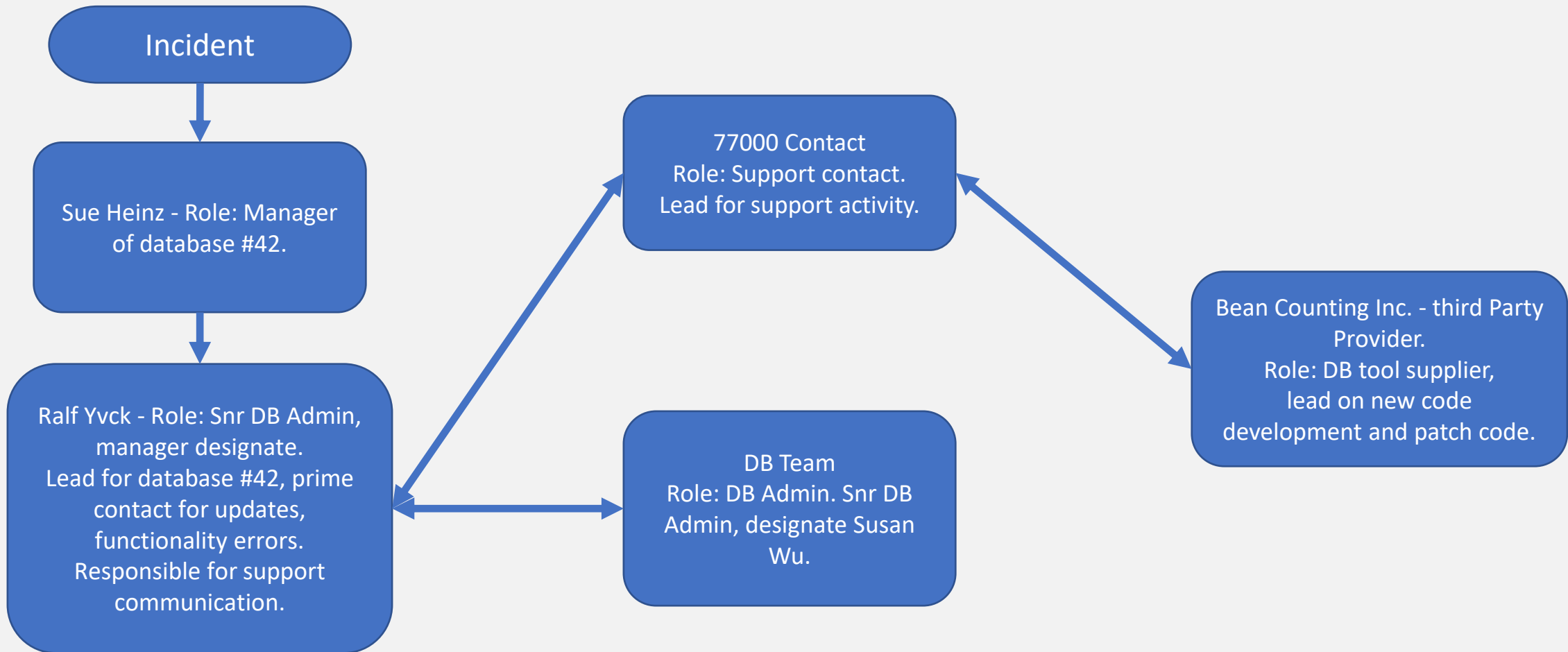
- The **roles and responsibilities**, the **who**.
- The **methods of communication**, the **how**.
- The **communication types**, the **what**.

Understanding the who, how, and what, allows for a faster response to incidents.



Example Organisation Communication Flow chart:

"Communications Flow - Database #42"



Fictional scenario.

Creating a Map of Organisational Data Flow Diagrams

Data Flow Diagrams (DFD) are used to graphically represent the flow of data in an information system. Think of them like LEGO instructions, taking you from one step to another. DFD describes the processes that are involved in a system in order to transfer data.

DFDs can be divided into both logical (which can be digital) and physical.

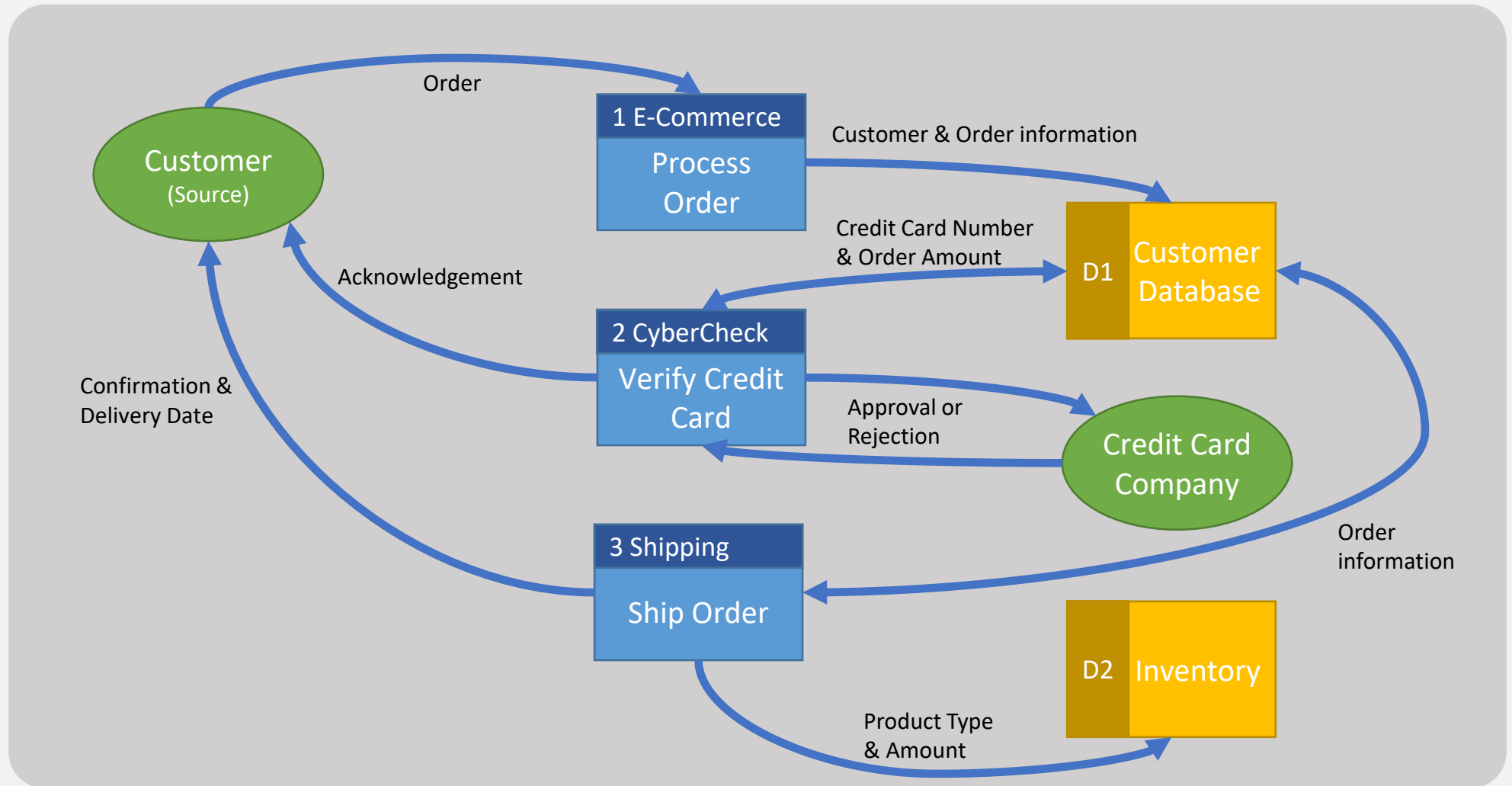
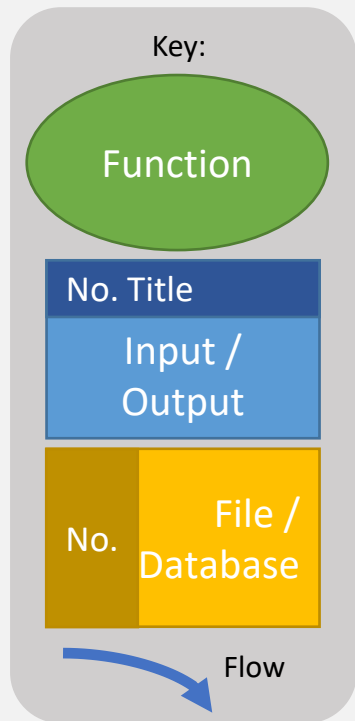
The logical data flow diagram describes flow of data, through a system, in order to perform business functions. The physical data flow diagram describes the physical implementation, the hardware, of a data flow.

For each data flow, at least one of the endpoints must exist in the process: Either the **source** or **destination**.



LEGO Stephen Hawking, black hole not included.
<https://www.brothers-brick.com/2017/03/31/standard-model-instructions/>

Example Data Flow Diagram – An Online Order System



Fictional scenario.



SITAM Goals



Secure IT Asset Management Goals

There are **three main overall goals** that should be kept in mind as a SITAM process is planned, these are:

Overall Goals

1. Plan and organise your devices.
2. Keep devices visible and healthy.
3. Retire devices.





1. Plan and organise your devices

Setup your asset management tools to reflect your business goals.

This means considering all of your devices, and document the purpose of each device. Also, document the expected lifespan of each device including the refresh cycles, lease date, or end of life warranty. This information comes back to the **who how and what** questions.

Establishing your users expectations before placing a device in their hands, this ensures that you can detect and control unexpected changes, or threats, as they happen. Which will minimise the impact on the business.

2. Keep devices visible and healthy

SITAM should create a baseline understanding of the environment. This allows devices to be monitored for their health, age, performance and risk.

We must understand what is in our environment. If we are unable to identify devices, and what it is they are doing, then how can we replace or renew them if something unexpected happens. For example, what happens when a device is lost or stolen? How will you know to replace it? Or what to replace it with?



3. Retire devices

All devices have a life cycle, which will include the **retirement of devices**.

Retirement means that retired devices are collected, secured, sanitised, and removed from our environment. This helps to prevent the appearance of ghost devices.

The accuracy of life cycle management will mean the incident response process will be faster, and more accurate. Some questions to consider are:

1. How will you manage device returns when employees leave or change roles?
2. How do you manage timely, and secure, device end-of-life?
3. How can you confirm that are they safely decommissioned from your organisation?

As the number of devices and the volume of the data in the government increases, it becomes increasingly critical to maintain visibility, and control, of assets. Proactive secure IT asset management is how you accomplish that goal.

See [Asset Related B.C. Government Policies Procedures and Standards](#) (internal link) later in this course for secure asset disposal procedures.





Defining Critical Assets

It is possible that any asset can become a critical asset, given the right circumstances. These assets could be informational assets, physical assets, people, or a software assets. **Critical assets are those where failure is serious enough to affect ongoing business operations.** For example, financial systems, business operations or other mission-critical systems.



Critical assets should have automatic systems monitoring them, so that the appropriate staff are alerted if an incident occurs. Critical assets might need to have redundancy, two people, or two servers, to undertake certain work, as this prevents a single point of failure.

It is important to make the distinction between the severe consequences of a critical asset's failure, versus the actual probability of it failing. Even if a critical asset failing might be disastrous, it doesn't mean that asset is any more likely to fail.

Note that when it comes to people, those who possess confidential and proprietary information, and whose absence would cause destabilisation within the business, measures should be taken to document this, and cross-train other staff, to prevent a single point of failure.

Critical assets should be documented as a part of the SITAM process. Ministries should collaborate on, or share the documentation of, critical assets. This should include the risk assessments for those assets. This will enable standardisation, time, effort, and provide cost savings.

The B.C. Government has a critical systems standard, as well as other standards and policies, that should be followed when defining a critical system. These are linked later in this course.



B.C. Government Critical Systems Standard & Guidelines

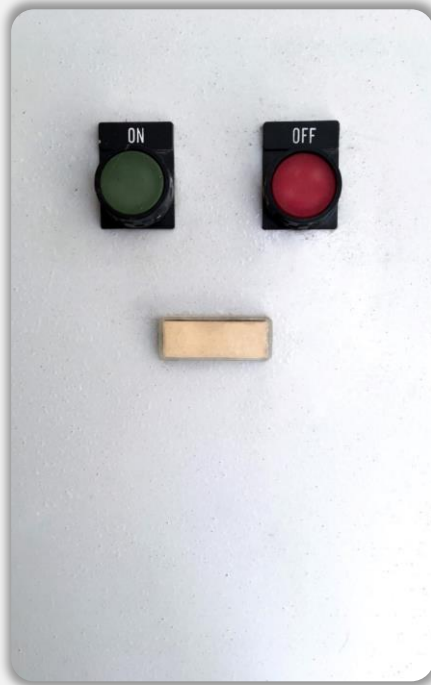
Critical Systems Standard

https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/criticalsystemsstandard_v30.pdf (PDF link)

“As the IM and IT operating environment continues to increase in scale, complexity, and dependencies, the risk of disruptions to business services become greater. The effect of a loss of a mission critical service on individuals can bring hardship, and possibly result in injury or even death.

This increased complexity demands higher levels of vigilance in our security posture and improved coordination to be successful in delivering stable services to citizens. Lessons learned from service interruptions in government and have pointed to ways of improving how we recognise and more effectively deal with these kinds of disruptions. This critical systems standard addresses the immediate concerns from lessons we have recently learned and also lays the foundations for a program of continuous improvement.”





Critical Systems Guidelines

These are linked off the main Policies and Procedures IM IT page, <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard>

This guidelines describe proposed approaches, actions, and documentation needed in the standard:

- Aiding in the interpretation of the standard.
- Outlining the minimum expectations of the specific requirements, as defined in the standard.





SITAM in the B.C. Government



ASSET MANAGEMENT SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0
Published: September 2019

SITAM Policies and Standards

The [Asset Management Security Standard](#)¹ is created and maintained by the Information Security Branch, which is part of the Office of the Chief Information Officer, within the Ministry of Citizens' Services.

The standard is designed to be read in conjunction with the Information Security Standard, as it is a sub-section of that standard.

This standard should be read in conjunction with [the Asset management Security Guideline](#)².



1. <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard>, PDF link
2. <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-guideline-policy>



Information and information systems services constitute valuable government resources.

The 'Asset Management Security Standard' establishes the rules of acceptable use, and protection. That is, what assets to protect, who protects them, and how much protection is required.

The standard also specifies a requirement to designate who owns the assets. Designated owners become responsible for protecting information, and technology assets, and to maintain the way those assets are protected.

Finally, the standard requires that assets are classified into different security levels. This helps to show how much protection is expected, and how information should be handled at each classification level.

Not all information requires the same level of protection, because only some information is sensitive or confidential. More details on information classification follow.

Asset owners responsibilities

It is important that the owners of assets fully understand the asset that they are protecting. Here are some guidelines for asset ownership:

- 1 Define responsibility for assets
- 2 Information Classification
- 3 Responsible for Removable Media

For all of the details please see the current [Asset Management Security Standard](#)¹, although this course will cover the topics in the standard, it will not go down to the same level of detail. The standard may change independently of this course.

Citizens' Services and Ministries should collaborate to periodically review and update core government policies and standards and ministry-specific guidelines in accordance with good information security practices regarding IT asset inventories.

1. <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard>

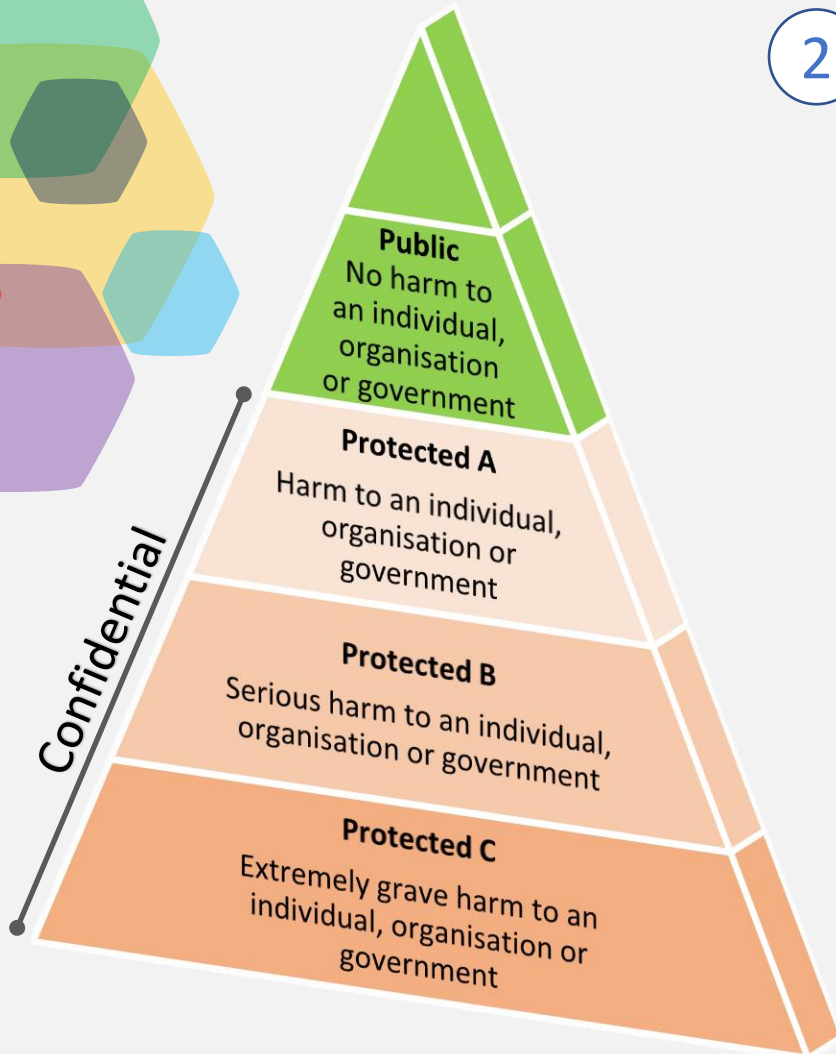
1

Asset Management Security Standard: **Responsibility for Assets**

1. An inventory of all important assets associated with information systems must be **documented and maintained**. To identify information assets and define appropriate protection responsibilities.
 - a) Identification of assets
 - b) Documenting and maintaining asset inventories
 - c) Loss, theft or misappropriation of assets
2. Information Owners and Information Custodians must be designated for all assets associated with information systems. To **designate custodians for assets**, with approved management responsibility, for the protection of organisational assets associated with information and technology systems or services.
 - a) Responsibilities for asset ownership
 - b) Designating Information Custodians
3. Rules for the **acceptable use** of information systems must be identified, documented and implemented. To prevent misuse or compromise of government information systems.
 - a) Acceptable use of government resources. To ensure employees return physical and information assets at termination or change of employment.
4. Employees must return government assets upon termination or change of employment.
 - a) Return of assets

2

Asset Management Security Standard: **Information Classification**




Information Classification Standard¹

1. <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-classification>

1. The government information security classification system must take into account the value, sensitivity and intended use of the information based on risk assessment. To **define** the information security classification system characteristics for information and information systems.
 - a) Information and information system security classification
 - b) Mandatory features of information security classification
 - c) Mandatory features of information system security classification
2. Information must be identified, labelled when appropriate and handled in accordance with the assigned information security classification. To **protect** information in accordance with its security classification.
 - a) Information labelling procedures
 - b) Information handling procedures
3. Information assets must be handled and stored so as to prevent unauthorized information disclosure or misuse, in accordance with the information security classification system. To ensure that documented procedures are used for handling information assets and **storage** of media in accordance with the security classification of information stored on the media.
 - a) Asset handling procedures
 - b) Media handling procedures

Asset Management Security Standard: Removable media

- [illegible]



The OCIO and the ministries must all work together to enable information sharing, and follow the government's standards and guidelines regarding secure asset management. We must work to identify, establish, and document cybersecurity roles and responsibilities for employees, and for third-party stakeholders, including where those persons have a role in managing IT assets.



The OCIO and the ministries must adopt a consistent approach for identifying and tracking IT assets to ensure the completeness and accuracy of inventories of IT assets. This is to ensure that asset inventories are complete and accurate, based on the assets' risk, and the ministries' individual risk appetite.

The Asset Management Standard and Guidelines create a central framework that standardises the approach to asset management across all of government. This allows for the sharing and reuse of asset risk assessments, and understanding of assets. This saves time, effort and allows for the faster assessment of asset risk with greater accuracy; effectively sharing the work load across the OCIO and the ministries.

Asset Related B.C. Government Policies, Procedures and Standards

Find and access policies and related services for the B.C. Government and the broader public sector on the Services for Policies for Government website located at: <https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures>. Directly related to Asset Management includes, but is not limited to, the following:

Travel with Mobile Device or Laptop

Guidance on the use of mobile devices given current legal requirements, government policy, and best practices. Many of the key requirements applicable to mobile devices come from the Appropriate Use Policy and the Information Security Policy. https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/policies-procedures/it-policies/mobile_device_guidelines.pdf

Asset Disposal Procedure

Disposal of any kind of tangible, surplus asset, contact AIR Customer Service (AIR.CustServ@gov.bc.ca) about your organisation's unique disposal needs – <https://www2.gov.bc.ca/gov/content/governments/services-for-government/bc-bid-resources/goods-and-services-catalogue/asset-recovery-disposal>

Creating a formal periodic review process for assets

All assets need to have a periodic formal review process defined and documented. Physical assets must have, at least, an annual review as defined in the Core Policies and Procedures Manual, Chapter 8 – <https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/policies/asset-management>.

Asset Related B.C. Government Policies, Procedures and Standards

Capital Asset Management Framework

Capital asset management planning is the process of identifying current and future capital needs, and developing strategies and projects to address those needs -

<https://www2.gov.bc.ca/gov/content/governments/policies-for-government/capital-asset-management-framework-guidelines/planning>

Critical Systems Standard

PDF Link:

https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/criticalsystemsstandard_v30.pdf

Asset Management Framework

<https://www.assetmanagementbc.ca/framework/>, Asset Management BC

PDF Link: <https://www.assetmanagementbc.ca/wp-content/uploads/Asset-Management-for-Sustainable-Service-Delivery-A-BC-Framework-.pdf>

Critical Systems Guidelines

PDF Link:

https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/css_guidelines_v30.pdf

Critical infrastructure assessment

<https://www2.gov.bc.ca/gov/content/safety/emergency-preparedness-response-recovery/local-emergency-programs/critical-infrastructure-assessment>



Summary



Summary

In this course we have learned what IT asset management is, and the differences when compared to secure IT asset management. The benefits of SITAM, both financial and organisational, have been clarified; a good SITAM program will act as both a canary, and a tool to aide a quicker recovery from an incident.

The most used SITAM framework is that created by NIST as a part of their overall Cybersecurity Framework, this course covers what defines the framework, the ten best practices of SITAM, and the desired outcome. As well as understanding the asset management lifecycle you should now be able to create an inventory record, communication and data flow and know the overall goal of SITAM.

The B.C. Government has a number of policies and standards that relate to SITAM, you should now understand what some of these are and how to access them. We here in the Information Security Branch hope this course have been of value to you!

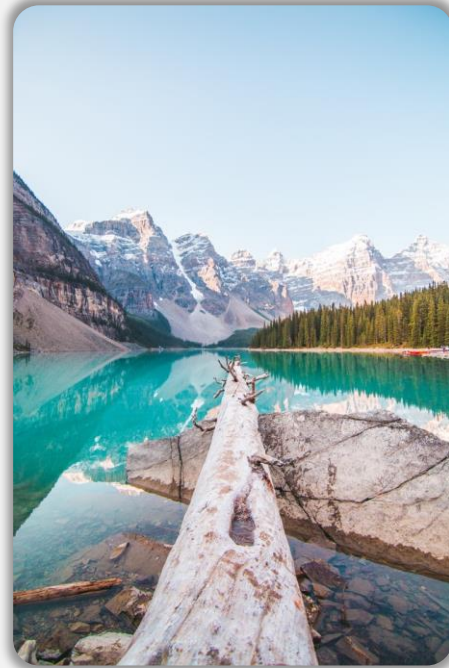


Thank you for your time
and energy in taking this
course, together we help
to secure British Columbia

Success!



Images and diagrams used in this course are created by the author, or are sourced from the following free image repositories, unless otherwise noted:



<https://pixabay.com/service/terms/#license>

“Under the Pixabay License you are granted an irrevocable, worldwide, non-exclusive and royalty free right to use, download, copy, modify or adapt the Content for commercial or non-commercial purposes. Attribution of the photographer, videographer, musician or Pixabay is not required.”

<https://www.piqsels.com/terms-of-service>

“The images provided by Piqsels are free to use for personal and commercial projects. Attribution is not required.”

<https://www.pexels.com/license/>

“All photos and videos on Pexels are free to use. Attribution is not required. You can modify the photos and videos from Pexels.”

<https://unsplash.com/license>

“Unsplash photos are made to be used freely. Our license reflects that. All photos can be downloaded and used for free. Commercial and non-commercial purposes. No permission needed.”