What is IT asset management (ITAM)?

IT asset management (also known as ITAM) is the process of ensuring an organization's assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes. Put simply, it's making sure that the valuable items, tangible and intangible, in your organization are tracked and being used.

So, what's an IT asset? Defined simply, an IT asset includes hardware, software systems, or information an organization values. In Atlassian's IT department, some of our most important assets are the computers and software licenses that help us build, sell, and support our software and the servers we host it on.

IT assets have a finite period of use. To maximize the value an organization can generate from them, the IT asset lifecycle can be proactively managed. Each organization may define unique stages of that lifecycle, but they generally include planning, procurement, deployment, maintenance, and retirement.   An important part of IT asset management is applying process across all lifecycle stages to understand the total cost of ownership and optimize the use of assets.

In the past, IT departments were able to control assets within their own domain. Now, an organization's asset management practice extends far beyond the hardware that's issued with an official IT stamp of approval. Subscription-based software and employees expectation to customize the tools they work with through marketplaces and app stores, present new asset management challenges. The way modern teams work requires that IT teams be flexible and adapt their asset management process to best enable the business.

As various teams push to work with the tools that best fit their needs, asset management is an even more important part of an organization's overall strategy and provides up-to-date information to reduce risks and costs. An asset management process creates a single source of truth when optimizing budgets, supporting lifecycle management, and making decisions that impact the entire organization.

As teams outside of IT begin to embrace service management, asset management has also become important to a variety of departments. We've heard of organizations using asset management software to manage things ranging from fleets, to fish, to insurance, to musical instruments.

Why is ITAM important?

Providing a single source of truth

Too often, assets get tracked in a ton of different places, by a ton of different people. No single person owns things, and no single tool collects and centralizes the information. Naturally, chaos and inaccuracy follow. It's difficult to make informed decisions. There are even companies where people are being employed just to keep track of IT assets. Systems should do this work. Without having to relegate time and brain matter to tracking artifacts, monitoring usage, and understanding dependencies, IT employees can focus more on what matters most to the organization. Asset management brings order, and offers a single source of truth for IT teams, management, and ultimately, entire organizations.

Improving utilization and eliminating waste

Asset management keeps information updated, so teams eliminate waste and improve utilization. It saves money by helping avoid unnecessary purchases and cutting licensing and support costs. Increased control also enforces compliance with security and legal policies and reduces risks. The positive implications on costs and productivity benefit the entire organization.

Enabling productivity without compromising reliability

With digital transformation changing the way organizations operate, modern asset management goes far beyond tracking laptops and mice. Teams are embracing DevOps and SRE principles, and need asset management processes and tools in order to efficiently deliver new functionality and services quickly without compromising on reliability. In the report Prepare Your IT Asset Management for 2020, Gartner notes that given the increased reliance on platform and infrastructure services, effective asset management can enable organizations to manage their consumption of "on-demand services." With increased control, visibility, and assigned responsibility, teams can reduce excess consumption including overprovisioning, and idle instances, avoiding unnecessary costs.

Supporting ITSM practices and enabling teams across organizations

IT asset management is critical to supporting ITIL processes, including change, incident, and problem management. The IT team enables the entire organization to get more innovative and deliver value more quickly. With the right data at their fingertips, teams can move with speed and predict the impact of changes before they happen. By democratizing access to insights, the organization gains a competitive edge, delivering value more quickly. Any organization trying to keep up with the pace of modern innovation needs to get strategic about controlling, tracking, and mastering IT data.

The IT asset management process

IT asset management is not a project. You don't do it once and expect it to be finished. ITAM is a process that teams execute on a regular basis or as assets, goals, and tools change.

1. **Inventory assets** - The first step in the IT asset management process is to create a detailed inventory of all IT assets. Your inventory includes what assets you have, where they are located when they were purchased, and for how much.

2. **Calculate lifecycle costs** - The second step is to calculate lifecycle costs for all assets in your inventory. During an average asset's life, there are many opportunities for added costs, like maintenance, capital, and disposal costs. Calculating lifecycle costs makes your asset inventory accurate and actionable.

3. **Tracking** - The third step is tracking via an asset management tool. Your goal is to continuously monitor IT assets through their lifecycle keeping a close eye on things like

contract, license, and warranty expiration. Tracking also helps you stay ahead of the fourth step, maintenance.

4. **Maintenance** - Maintenance involves asset repair, upgrade, and replacement. All maintenance activities should be tracked in an ITAM tool so that the data can be used to understand the overall performance of the asset.
5. **Financial Planning** - The fifth and final step is financial planning. With an accurate picture of your IT assets, their lifecycle stage, and their costs, you can effectively plan for the future. One goal of financial planning is to determine the budget needed to maintain or improve the "levels of service" your team provides for your most important assets. An asset that was successfully managed with a high level of service, like a service desk and dedicated team, will need that level of service going forward. Assets that underperformed may need a higher level of service in the future, which will cost more.

"Maintenance of IT assets" refers to the process of regularly inspecting, servicing, and repairing an organization's Information Technology (IT) equipment, like computers, servers, printers, and software licenses, to ensure they remain functional and operate optimally throughout their lifespan; this includes preventative measures, updates, and addressing issues as they arise, all while tracking asset details for effective management.

Key aspects of IT asset maintenance:

- **Asset tracking:**

Keeping a detailed inventory of all IT assets, including their location, condition, and warranty information.

- **Preventative maintenance:**

Performing regular checks and updates to identify potential problems before they cause major disruptions, like software patching, hardware diagnostics, and cleaning routines.

- **Software updates:**

Regularly installing the latest software patches and updates to address security vulnerabilities and improve performance.

- **Hardware upgrades:**

Planning and executing hardware upgrades when necessary to maintain optimal performance and compatibility with newer technologies.

- **Data backup and recovery:**

Implementing robust data backup procedures to protect critical information in case of hardware failure.

- **Compliance management:**

Ensuring IT assets adhere to relevant industry regulations and standards regarding data privacy and security.

- **Lifecycle management:**

Tracking the lifecycle of each asset from procurement to disposal, including decommissioning and proper asset retirement processes.

Benefits of effective IT asset maintenance:

- **Reduced downtime:**

Proactive maintenance helps prevent unexpected system outages and disruptions to business operations.

- **Cost optimization:**

Identifying potential issues early can prevent costly repairs and extend the lifespan of assets.

- **Improved productivity:**

Reliable IT infrastructure ensures employees can work efficiently without technical interruptions.

- **Enhanced security:**

Regular updates and patching help mitigate security risks and protect sensitive data

End-of-Life (EOL)

- The date when a product is no longer sold or renewed
- The date when a product line and its accessories are no longer manufactured

End-of-Support (EOS)

- The date when a manufacturer stops providing technical support and updates for a product
- The date when a product will no longer receive security updates

What's important about EOL and EOS?

- It's important for companies to understand EOL and EOS so they can switch to new solutions in a timely manner.
- Using products that have reached EOL or EOS can expose a company to security vulnerabilities, legal risks, and financial risks.
- Companies should create and implement a plan before the end of support dates.

End of Maintenance (EOM) is the date when a product or service will no longer receive updates, bug fixes, or security patches.

What happens after EOM?

- **No more updates**

After EOM, the product will no longer receive updates, bug fixes, or security patches.

- **No more security advisories**

Users will lose access to security advisories and urgent bug fix advisories.

- **Migration to new solution**

Users will need to migrate to a new solution to continue receiving support, updates, and security fixes.

How to plan for EOM?

- **Plan next steps**: Plan ahead to avoid gaps in coverage and ensure continuous operation.
- **Evaluate new equipment**: Consider whether new equipment is needed, and the cost of operating older equipment.
- **Engage stakeholders**: Communicate the reasons for the transition, and how changes will affect different departments.
- **Oversee implementation**: Ensure new technology integrates well with existing systems and processes.

Asset hygiene refers to the proper management, maintenance, and security of digital and physical assets to ensure they remain functional, secure, and up to date. It applies to IT assets (like software, hardware, and cloud resources) as well as physical assets (like machinery and equipment).

Key Aspects of Asset Hygiene:

1. **Inventory Management** – Keeping an updated list of all assets.
2. **Regular Updates & Patching** – Ensuring software, firmware, and hardware are updated.
3. **Access Control** – Limiting access based on roles and necessity.
4. **Security Measures** – Using firewalls, antivirus, and encryption.
5. **Compliance & Auditing** – Ensuring regulatory and company policy compliance.
6. **End-of-Life Management** – Properly decommissioning outdated assets.

In cybersecurity, a "**crown jewel**" refers to an organization's most critical and valuable asset, like sensitive customer data, proprietary intellectual property, or mission-critical systems, which if compromised would cause significant damage to the company's operations, reputation, and finances; essentially, the data or systems that need the highest level of security protection.

Key points about crown jewels in cybersecurity:

- **High impact potential:**

A breach of crown jewel data could lead to major financial loss, regulatory issues, or significant reputational damage.

- **Specific to each organization:**

What constitutes a crown jewel varies depending on the company's industry, business model, and critical information.

- **Requires robust security measures:**

Crown jewels should be protected with the most stringent security controls, including encryption, access controls, and constant monitoring. s

Examples of crown jewels in different industries:

- **Financial institutions:** Customer account details, credit card informationf, trading algorithms
- **Healthcare providers:** Patient medical records, insurance details, genetic data
- **Retail companies:** Customer purchase history, loyalty program data, credit card details
- **Tech companies:** Source code, intellectual property, trade secrets

Inventory

In cybersecurity, an "inventory" refers to a comprehensive list of all an organization's digital assets, including hardware, software, network components, data, and even user accounts, essentially creating a detailed catalog of everything connected to the network that needs to be secured, allowing for better risk assessment and proactive security measures by understanding the entire "attack surface" of the organization. s

Key points about cybersecurity inventory:

- **Foundation of security programs:**

An accurate asset inventory is considered the fundamental building block of a robust cybersecurity strategy, as it provides visibility into potential vulnerabilities and areas that require focused security attention.

- **What it includes:**
    - Physical devices like computers, servers, IoT devices

- Software applications and operating systems
- Network components like routers and switches
- Data stored on systems
- Cloud environments and virtual machines

NVD

The **National Vulnerability Database** (NVD) is a repository of vulnerability management data for the U.S. government. It's a key resource for cybersecurity professionals to identify and mitigate cyber threats.

What does the NVD do?

- Centralizes vulnerability data from security researchers, vendors, and other sources
- Provides standardized data on software and hardware flaws
- Helps security teams quickly identify vulnerabilities and prioritize remediation
- Enables automation in vulnerability management workflows

What does the NVD include?

- Databases of security-related software flaws, misconfigurations, product names, and impact metrics
- Entries for Common Vulnerabilities and Exposures (CVEs), which include descriptions, severity scores, and references to related advisories or solutions

How can organizations use the NVD?

- To prioritize vulnerabilities and patches to keep their IT infrastructure safe
- To automate vulnerability management, security measurement, and compliance

Who maintains the NVD?

- The National Institute of Standards and Technology (.gov) (NIST)

Patch management

Patch management is a process that updates software to fix vulnerabilities and improve functionality. It's a key part of cybersecurity because it helps protect systems from hackers and data breaches.

What does patch management do?

- Corrects errors, also called bugs or vulnerabilities
- Improves functionality

- Ensures compliance
- Resolves threat vectors that hackers might use to access sensitive information

How does patch management work?

1. **Identify**: Find out which software needs updating
2. **Acquire**: Get the updates
3. **Test**: Make sure the updates are safe to deploy
4. **Deploy**: Install the updates
5. **Verify**: Check that the updates are working

What are the different types of patches?

- **Security patches**: Fix security vulnerabilities
- **Bug-fixing patches**: Fix bugs in the software
- **Feature updates**: Update the features of the software

Why is patch management important?

- It helps protect systems from hackers and data breaches
- It can reduce the number of critical patches that go unapplied