ApexaIQ Day 1

* IT Assets:

An asset is something you own that plays a role in helping you conduct your day-to-day business operations. However, the term IT asset refers to the domain and includes everything you own that helps you perform computer-based tasks.

Any piece of hardware, software or digitally stored information that holds value for your business qualifies as an IT asset. Let’s look at the different types of IT assets to have a better understanding.

* **Hardware**– Any object that has a chip inside of it and helps you conduct digital tasks is IT hardware. For instance, laptops, smartphones, mice, keyboards, printers, Wi-Fi routers, and telephones. Note that hardware is not limited to these objects only.
* **Software –**Software that helps you conduct your business operations, such as your invoicing system, is also considered an IT assets.

**Digital Information**– Any information of value stored on a computer or an online database is an IT asset. These could be financial datas heets, licence agreements, and even [NFTs or crypto assets](https://itemit.com/nft-cryptocurrency-iot-asset-tracking/).

* IT Asset Management:

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.  IT asset management (ITAM) empowers IT teams to manage the full lifecycle of a company’s IT assets, with the goal of achieving a higher return on investment (ROI) and security posture for the business.

* Vulnerability:

Vulnerability refers to the weakness or flaw in a piece of IT hardware or software that could be exploited by the cyber attackers to gain unauthorized access to a system, to steal data or disrupt operations.

* Obsolescence:

Obsolescence in IT Asset Management refers to the point when an IT asset—be it hardware, software, or digital infrastructure—becomes outdated, no longer supported, or no longer meets current business needs. Obsolete assets can pose risks, increase costs, and hinder operational efficiency.

* Compliance:

Compliance refers to the practice of following legal regulations, industry standards, and internal policies that govern the management and use of IT Assets ensuring that all the assets are being handled according to established guidelines to avoid legal cases and maintain data security.

* Maintenance:

Maintenance refers to the process of managing, repairing, upgrading, and replacing IT assets throughout their lifecycle. It is also analysing the performance of IT Asset and make informed decisions according to it for the better efficiency of the business.

* End of Life:

End of life refers to the stage where a piece of hardware or software reaches to the end of its lifespan and is no longer supported by the vendor or manufacturer, meaning it will not receive any further update, maintenance or should be retired.

* End of Support:

End of support refers to the stage where the manufacturer stops giving support to any IT asset, be it hardware or software, essentially marking the end of its lifecycle for the better version and security.

* End of Maintenance:

End of maintenance refers to the stage where the vendor stops providing and maintenance support and updates to the IT asset, be it hardware or software, essentially marking the end of its useful life and signifying that the company will no longer actively maintain that product, leaving users vulnerable to security risks and potential issues without updates.

* Crown Jewel:

Crown Jewel refers to the most critical and valuable asset in the organization, meaning the system, data or application that would cause the most significant disruption if compromised, thus requiring the highest level of security and protection compared to other assets.

* Asset Hygiene:

Asset hygiene refers to the practice of maintaining a clean and accurate record of all the IT asset within an organization, ensuring the asset information is up to date, cleaned and free from errors.

* Inventory:

IT asset inventory is the process of identifying, tracking, and managing all **hardware and software assets** an organization owns or uses. This includes servers, laptops, mobile devices, printers, network devices, software licenses, and other technology-related items contributing to the organization's [**IT infrastructure**](https://blog.invgate.com/it-infrastructure).

* NVD:

The National Vulnerability Database (NVD) is a foundational cybersecurity resource that provides detailed information on vulnerabilities across a wide range of software and hardware. Maintained by the National Institute of Standards and Technology (NIST), the NVD serves as the U.S. government repository of standards-based vulnerability management data. For security professionals, the NVD offers an invaluable source of actionable data to identify and mitigate cyber threats.

* Patch management:

Patchmanagement is the process of identifying, acquiring, testing, and applying updates (called "patches") to software, systems, and applications in an IT environment to correct issues or vulnerabilities. These patches are often released by software vendors to improve security, fix bugs, or enhance functionality.