IT Asset Management (ITAM)

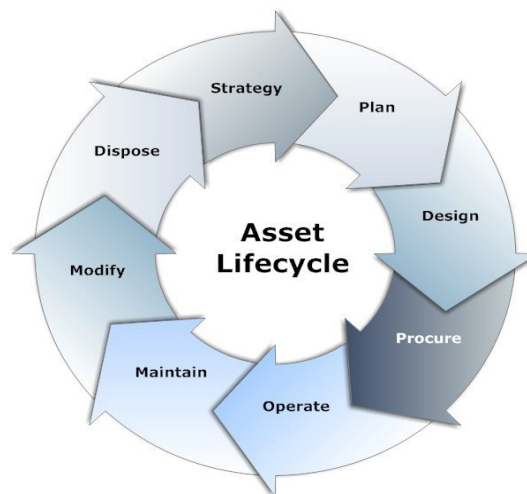## Why is IT asset management so important?

Financial institutions are built around technology; therefore, it can be a real challenge to keep track of it all. As institutions continue to embrace technology for everyday operations, it becomes more and more critical to establish and maintain a firm handle on all assets in the institution's environment. An effective **IT asset management (ITAM) program** that manages all aspects of the asset life cycle is a cornerstone control that:

- Supports institutional risk management, including the development and maintenance of the information security program;
- Helps to enable the effective design, implementation, and troubleshooting of technology solutions and the mechanisms to secure them;
- Strengthens the effectiveness and comprehensiveness of patch management efforts; and
- Helps to ensure that end-of-life assets are properly identified and managed.

> *It is impossible for an institution to manage assets it does not know it has.*

The IT asset life cycle

All IT assets – software, hardware, mobile devices, cloud assets, etc.- have a lifecycle. The following illustration from NIST[1] provides a top-level overview of the lifecycle stages for IT assets.

Graphic Source: NIST

The lifecycle begins with strategies and planning for acquiring or developing the asset and continues logically through the ongoing operation and maintenance of the asset, as well as any potential

---

[1] National Institute of Standards and Technology. NIST Special Publication 1800-5B, IT Asset Management, Volume B: Approach, Architecture, and Security Characteristics. September 2018.

modifications that may be necessary over the course of its lifespan. The final stage of the lifecycle addresses the proper disposal of the asset at the end of its useful life.

ITAM and risk management

Effective ITAM is a critical contributor to effective risk management practices throughout the institution. Robust technology asset inventories can assist in the **development of risk assessments** (e.g., information security, SOX, continuity and resilience, business unit, etc.) and can assist in compiling **audit risk assessments** and **building the audit universe and scope**.[2]

According to the FFIEC IT Handbook booklet: *Architecture, Infrastructure, and Operations, "*Management should have a comprehensive inventory of its electronic (or digital) and physical information assets to **adequately safeguard them against reasonably foreseeable threats**. An inventory will assist management as it develops and maintains the entity's **information security program** as described in the Information Security Standards."

ITAM helps to:

- Enable informed decision making required for **long-term planning**. When management is aware of its current inventory, they can better assess necessary design changes while ensuring that strategic goals align with the institution's distinct mission.
- Enable the **identification and acquisition of hardware and software that integrates best with the company's existing infrastructure**. This ensures both smooth scalability and avoids unnecessary business disruptions.[3]

Finally, effective ITAM processes and scanning tools can help to identify unauthorized IT devices, software, or other services, known as **"shadow IT,"** operating within the entity's environment or inside a third-party service provider's environment. According to the FFIEC, "Failure to address the risks of shadow IT may lead to an unknown attack vector due to management's lack of awareness of unapproved devices, software, or services." These risks may include, but are not limited to, security weaknesses, breaches, or loss of data from unapproved technology; an inability to accurately maintain and update shadow IT assets; and unintentionally backing up unmanaged devices, which may lead to the proliferation of malware throughout the network.[4]

ITAM is a foundation for vulnerability, patching, and end-of-life management programs

According to the FFIEC, "ITAM inventories help management know what systems need to be patched and the patch time frames, what hardware or software is nearing end-of-life, where the entity's vulnerability management focus should be, or when any additional security measures are necessary."[5]

---

[2] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1 - Technology Asset Inventory. June 2021.
[3] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B - IT Asset Management. June 2021.
[4] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.3 - Shadow IT. June 2021.
[5] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B - IT Asset Management. June 2021.

Threat actors can quickly capitalize on even temporarily unpatched vulnerabilities in both software and hardware assets. Comprehensive, dynamically updated inventories of technology assets can help to make vulnerability identification and patching efforts more thorough, expedient, and effective. In fact, the success of the institution's patch management program is dependent, in part, on maintaining a dynamic, accurate inventory of assets that captures <u>all new and existing technology assets making temporary or permanent connections to the network</u>. Periodically reconciling detailed inventories of hardware and software assets is a form of version control that helps to ensure that patch management efforts are comprehensive and function properly.

ITAM processes can also ensure that any **end-of-life (EOL) assets** can be identified and managed appropriately within the institution. Because EOL assets are not supported by current security patches and updates from the vendor, they can introduce significant cyber risk. Moreover, EOL assets that are mission-critical systems require significant lead time to allow for the identification of acceptable mitigations and plans for replacement. An accurate inventory can, at a minimum, provide the institution with an accurate view of where these unsupported assets might be present and introducing unacceptable or unknown security risks.

ITAM considerations for hardware and software

A crucial component of asset inventory management is the **categorization of systems**. For hardware, it is important to differentiate between inventory owned and managed by third parties or owned and managed in house. Proper tracking of these assets includes assigning each one a unique identifier, such as serial numbers or asset tags. In addition, to classification of hardware, information about the entity's network and telecommunications equipment should be accounted for.[6]

Software inventory should also be kept accurate, providing detailed information about various applications and systems in use across the entity. This includes details such as, but not limited to, application criticality, version numbers, licensing details, patch level and patching date, and alignment of deployment status with licensing agreements.[7]

Depending on the size and complexity of the institution, **the methods and tools used to manage the hardware and software inventories will vary**. According to the FFIEC, "There are tools that may help management identify and manage hardware (including telecommunications) and software in the entity's IT environment. For example, automated asset management tools can scan an entity's IT environment for unauthorized hardware, software, and devices. Smaller or less complex entities may use manual asset inventory processes; these processes, however, should allow management to effectively document, track, and oversee the entity's technology assets."[8]

[6] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1(a) - Hardware Inventory. June 2021.
[7] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1(b) - Software Inventory. June 2021.
[8] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook: Architecture, Infrastructure, and Operations - III.B.1 - Technology Asset Inventory. June 2021.

CONFERENCE OF STATE BANK SUPERVISORS
1129 20th Street NW / 9th Floor / Washington, DC 20036 / p: (202) 296-2840 / f: (202) 296-1928
www.csbs.org
@csbsnews