

# Asset Lifecycle Document (IT Asset Management - ITAM)

## Policy Statement

World Bank shall implement and maintain a comprehensive Information Technology Asset Management (ITAM) program. This program will systematically track, manage, and secure all IT assets throughout their entire lifecycle, from initial planning and procurement through deployment, operation, maintenance, and eventual secure disposal. The ITAM program is essential for ensuring operational efficiency, optimizing IT investments, maintaining a robust security posture, and adhering to all legal, regulatory, and contractual obligations.

## Scope

This policy applies to all Information Technology (IT) assets owned, leased, or otherwise controlled by World Bank, irrespective of their physical location (on-premises, cloud, remote worker locations). This includes, but is not limited to :

- **Hardware Assets:** Servers (physical and virtual), desktop computers, laptops, mobile devices (smartphones, tablets), network equipment (routers, switches, firewalls, access points), storage devices (SAN, NAS, DAS), peripherals (printers, scanners), and IoT devices.
- **Software Assets:** Licensed commercial software, internally developed custom applications, open-source software, operating systems, middleware, and firmware.
- **Data Assets:** While data itself is managed under the Data Governance and Data Retention Policies, the ITAM program tracks the systems and media where data is stored, processed, and transmitted.
- **Cloud Assets:** Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) instances and subscriptions. Management of cloud assets also considers shared responsibility models.

## Roles and Responsibilities

Effective ITAM requires clear roles and responsibilities across various departments:

- **Asset Owners:** Typically senior managers or department heads who are accountable for the business use, justification, and risk associated with IT assets within their operational domain. They are responsible for approving access to their assets and ensuring assets are used in compliance with Bank policies.
- **ITAM Manager/Team:** Responsible for the overall governance, strategy, and operational management of the ITAM program. This includes maintaining the central IT asset inventory (often part of a Configuration Management Database - CMDB), developing and enforcing ITAM procedures, conducting audits, and reporting on asset status and compliance.

- **Procurement Department:** Responsible for the acquisition of IT assets in accordance with World Bank's procurement policies, technical standards, and security requirements. This includes vendor selection and contract negotiation.
- **IT Operations Department:** Responsible for the physical deployment, configuration, ongoing maintenance, patching, and technical support of hardware and software assets. They also manage the decommissioning of hardware.
- **Cybersecurity Team:** Defines security requirements and baselines for IT assets, assists in risk assessments of assets, provides guidance on secure configurations, and oversees the secure data sanitization and disposal processes.
- **Finance Department:** Tracks financial aspects of IT assets, including purchase costs, depreciation, and value for accounting and budgeting purposes.
- **Legal and Compliance Departments:** Provide guidance on legal, regulatory, and contractual obligations related to IT assets, including licensing, data privacy, and disposal requirements.

## Asset Lifecycle Stages & Procedures

The ITAM program at World Bank manages assets through the following distinct lifecycle stages :

- **1. Planning & Requirement Definition:**
  - Business units identify the need for new IT assets or the replacement of existing ones based on operational requirements, strategic projects, or technology refresh cycles.
  - Detailed technical specifications, functional requirements, and security requirements (e.g., encryption capabilities like FIPS 140-2 validation, secure boot, support for MFA) are defined in collaboration with IT, Cybersecurity, and relevant business stakeholders.
  - A budget is allocated, and a business case is developed for significant asset acquisitions.
  - *Security Manager's Perspective:* For any IT asset designated to store, process, or transmit World Bank's "Restricted" or "Confidential" financial data (as per our Data Classification Policy), FIPS 140-2 validated encryption for data at rest and in transit is a mandatory technical requirement during the planning phase. This proactive security stance is crucial for protecting our most sensitive information.
- **2. Procurement & Acquisition:**

- Vendors are selected based on a formal due diligence process, which includes an assessment of their security practices, financial stability, and ability to meet World Bank's technical and contractual requirements (refer to Vendor Risk Assessment Policy).
- Purchase orders and contracts must clearly articulate security obligations, licensing terms, support agreements, and, where applicable, rights to audit and secure disposal requirements.
- Upon receipt, assets are physically inspected, verified against purchase orders (model, quantity, specifications), and checked for any signs of tampering.
- *Use Case (Secure Procurement of Servers):* World Bank is procuring new high-performance servers for its primary data center to support an upgraded core banking application. The procurement process involves:
  1. Defining server specifications that include hardware security modules (HSMs) for key management, Trusted Platform Modules (TPM) for boot integrity, and capabilities for full-disk encryption.
  2. Issuing an RFP that mandates vendors provide attestation of their supply chain security practices to mitigate risks of hardware tampering or embedded malware.
  3. Evaluating vendor responses based not only on cost and performance but heavily on their security features and documented secure development/manufacturing processes.
  4. The selected vendor's contract includes clauses for timely security patch notifications and support for firmware updates.

- **3. Deployment & Installation:**

- **Asset Tagging:** Each physical asset is assigned a unique, tamper-evident asset tag (e.g., barcode, RFID tag) for identification and tracking.
- **Inventory Registration:** All new assets are immediately registered in World Bank's centralized IT Asset Inventory system (which may be integrated with a CMDB). Key data fields to be captured include : Asset ID, Asset Name/Hostname, Category (Hardware/Software/Data/Cloud), Description, Manufacturer, Model, Serial Number, Asset Owner (Department/Individual), Custodian, Physical Location (Building, Floor, Room, Rack), Network Configuration (IP Address, MAC Address), Operating System & Version, Key Installed Software, Purchase Date, Vendor, Warranty Expiration Date, Data Classification Level of primary data handled, Current Status (e.g., In Stock, In Use, In Repair, Awaiting Disposal), Security Baseline Applied.

- **Secure Configuration:** Assets are configured according to World Bank's approved Secure Configuration Baselines before being connected to the network or deployed for use. This includes hardening operating systems, disabling unnecessary services and ports, changing default credentials, and applying initial security patches.
  - **Software Installation:** Only approved and licensed software is installed. Security agents (e.g., Endpoint Detection and Response - EDR, Data Loss Prevention - DLP, MDM/UEM agents for mobile devices) are deployed as per policy.
  - **Network Integration:** Assets are connected to the appropriate network segment based on their function and security requirements.
- **4. Operations & Maintenance:**
    - **Monitoring:** Asset performance, utilization, and security status are continuously monitored. Automated tools are used to track asset health and detect anomalies.
    - **Patch Management:** Regular application of security patches and software updates is mandatory, following the Vulnerability Management and Patch Management Policies.
    - **Audits:** Periodic physical and logical audits of IT assets are conducted to verify the accuracy of the asset inventory, confirm physical locations, ensure compliance with security configurations, and identify any unauthorized assets or software.
    - **Software License Management:** Software licenses are actively managed to ensure compliance with vendor agreements and to optimize software expenditure. Unauthorized software installations are identified and remediated.
    - **Change Management:** Any changes to asset configurations, software, or location must follow the formal Change Management Policy.
    - **Movement Tracking:** All physical movements of assets between locations or reassignments between users/departments are tracked and updated in the IT Asset Inventory.
    - *Security Manager's Perspective:* World Bank employs a sophisticated suite of automated discovery tools that continuously scan our networks. These tools integrate directly with our CMDB, providing a near real-time, dynamic view of all connected assets. Any discrepancies, such as an unauthorized device appearing on the network or a critical server deviating from its security baseline, trigger immediate alerts to the SOC for investigation.

- **5. Redeployment / Reassignment:**

- When an asset is to be redeployed to a different user or for a different purpose, all sensitive data residing on it must be securely wiped in accordance with NIST SP 800-88 guidelines (typically "Clear" or "Purge" method, depending on data sensitivity).
- The asset is reconfigured to the standard baseline for the new user/purpose.
- The IT Asset Inventory records are updated to reflect the new owner, custodian, location, and configuration.

- **6. Disposal & Retirement:** This is a critical phase for security and compliance.

- **Identification & Approval:** Assets are identified for disposal when they reach end-of-life (EOL), end-of-support (EOS), become obsolete, are irreparably damaged, or are no longer required for business purposes. Formal approval for disposal is obtained from the Asset Owner and ITAM Manager.
- **Data Retrieval/Migration:** Before disposal, any business-critical data remaining on the asset must be securely backed up or migrated to a new system, in line with the Data Retention Policy.
- **Secure Data Sanitization:** All storage media (HDDs, SSDs, USB drives, backup tapes, mobile device storage) within assets slated for disposal *must* be securely sanitized to render data unrecoverable. World Bank mandates adherence to NIST SP 800-88 "Guidelines for Media Sanitization".
  - For assets that contained "Confidential" or "Restricted" World Bank data, a "Purge" or "Destroy" method is mandatory. This may involve cryptographic erasure, degaussing (for magnetic media), or physical destruction (shredding, disintegration).
  - The "Clear" method may only be used for assets that handled solely "Public" or "Internal Use Only" data with low sensitivity, and only if the asset is being reused internally within a secure environment.
- **Physical Disposal:** Hardware is disposed of in an environmentally responsible manner through certified e-waste recycling vendors who also provide certified data destruction services.
- **Inventory Update:** The IT Asset Inventory is updated to reflect the asset's "Disposed" status, including the date of disposal, method of data sanitization, method of physical disposal, and reference to any certificates of destruction or sanitization.

- **Documentation:** Maintain auditable records of all disposal activities, including chain-of-custody documentation if assets are handled by third-party disposal vendors, and certificates of data destruction/sanitization.
- *Use Case (Server Decommissioning and Secure Disposal):* A World Bank application server, which previously processed loan application data (classified as "Restricted"), is being retired due to an infrastructure upgrade.
  1. **Data Backup & Migration:** The Application Owner confirms that all active loan application data has been migrated to the new server platform and that historical data on the old server has been archived in accordance with the Data Retention Policy.
  2. **Network Disconnection:** The server is physically disconnected from the network. Its IP addresses, DNS records, and firewall rules are removed through the Change Management process.
  3. **Data Erasure (Purge):** The server's hard disk drives (HDDs) are removed. Each HDD is subjected to a degaussing process by the internal IT Operations team, following NIST SP 800-88 "Purge" guidelines. SSDs, if present, would undergo cryptographic erasure.
  4. **Physical Destruction (Destroy):** Following degaussing, the HDDs are sent to a certified third-party ITAD vendor contracted by World Bank. The vendor performs physical shredding of the drives.
  5. **Documentation & Inventory Update:** The ITAM team receives a Certificate of Destruction from the vendor, detailing the serial numbers of the shredded drives. The server's record in the IT Asset Inventory is updated to "Disposed," with the sanitization method (Degauss + Shred), disposal date, and Certificate of Destruction ID attached to the record. The physical server chassis is sent for e-waste recycling.

## Framework Alignment

This ITAM policy and its procedures are aligned with:

- **ISO 27001/ISO 27002:** Primarily Annex A.8 (Asset Management), which covers inventory of assets, ownership of assets, acceptable use of assets, and return of assets. Controls like A.7.10 (Storage Media in ISO 27001:2022, formerly related to A.8.3.1, A.11.2.7 in 2013) and A.8.10 (Information Deletion in ISO 27001:2022, relevant to secure disposal) are also pertinent.
- **NIST Special Publication 1800-5 (IT Asset Management for the Financial Services Sector):** This guide provides a reference architecture and practical guidance for ITAM, emphasizing centralized monitoring and lifecycle management, which World Bank's ITAM program emulates.

- **NIST Special Publication 800-88 (Guidelines for Media Sanitization):** This is World Bank's mandated standard for all data sanitization activities during asset redeployment and disposal.
- **FFIEC Guidelines:** The FFIEC emphasizes the importance of maintaining accurate IT asset inventories and secure lifecycle management practices for financial institutions to manage operational and cybersecurity risks effectively.

## Real-World Example: Laptop Refresh Cycle

A World Bank financial analyst's laptop, issued three years ago, is flagged by the ITAM system as due for a technology refresh.

- **Planning:** The ITAM system automatically generates a ticket. The standard laptop model for financial analysts is identified.
- **Procurement:** A new laptop, meeting current security specifications (e.g., TPM 2.0, full-disk encryption enabled by default, latest OS version), is ordered from an approved vendor.
- **Deployment (New Laptop):** Upon arrival, the new laptop is tagged, its details (serial number, model, etc.) entered into the IT Asset Inventory, and assigned to the analyst. It is configured with World Bank's standard secure operating environment (SOE), including security software (EDR, DLP, VPN client), productivity applications, and specific financial modeling software licensed to the analyst. Data from the old laptop is migrated securely.
- **Asset Return (Old Laptop):** The analyst returns the old laptop to the IT support desk. The return is logged against the asset record.
- **Disposal (Old Laptop):**
  1. The IT support team first performs a data backup verification to ensure all user data has been successfully migrated.
  2. The hard drive of the old laptop is then securely sanitized using a software-based "Purge" method (e.g., cryptographic erase if an SSD, or multiple-pass overwrite for older HDDs) compliant with NIST SP 800-88. This process is logged.
  3. The asset record is updated to "Sanitized - Awaiting Physical Disposal."
  4. The physical laptop is collected by World Bank's certified e-waste and data destruction vendor.
  5. The vendor provides a Certificate of Destruction for the hard drive (if physically destroyed after purging) and a Certificate of Recycling for the laptop components.

6. The IT Asset Inventory is updated to "Disposed," and the certificates are attached to the asset record.

**Table: IT Asset Register - Key Fields**

Field Name	Example Value / Description	Purpose & Importance for World Bank
Asset ID	WB-HW-LT-00789	Unique identifier for tracking and auditing. Essential for accountability.
Asset Name/Hostname	WBLON-FA-LT01 / ServerXYZ	Common name for easy identification by users and IT staff.
Category	Hardware, Software, Data, Cloud Service	Facilitates grouping, policy application, and reporting.
Type	Laptop, Server, Oracle DB License, AWS S3 Bucket	More granular classification for specific management procedures.
Description	Dell Latitude 7400, 16GB RAM, 512GB SSD / Oracle Database Enterprise Edition v19c License / S3 Bucket for Project Finance Archives	Brief details of the asset's specifications or purpose.
Asset Owner (Business Unit)	Department of Treasury Operations	Accountable business unit for the asset's use and justification.
Custodian (User/Team)	John Doe / Server Operations Team	Individual or team responsible for the day-to-day operational use or management.
Physical Location	London Office, Room 301 / Data Center A, Rack U25	Critical for physical security, audits, and recovery.
Status	In Use, In Stock, In Repair, Awaiting Disposal, Disposed	Current stage in the asset lifecycle, vital for planning and security.
Purchase Date	2023-03-15	Used for warranty tracking, depreciation, and refresh cycle planning.
Supplier/Vendor	Dell Inc. / Oracle Corp.	Important for support, warranty claims, and vendor management.
Warranty Expiry Date	2026-03-14	Triggers maintenance reviews and replacement planning.
Data Classification	Restricted, Confidential, Internal Use Only, Public	Determines the level of security controls required for the asset, especially if it stores or processes data. Critical for financial institutions.
Network Configuration	IP: 10.1.5.20, MAC: 00:1A:2B:3C:4D:5E	Essential for network management, security monitoring, and incident response.
Installed Software (Hardware)	Windows 10 Ent, Office 365, SAP Client, CrowdStrike Falcon	Important for license compliance, vulnerability management, and support.
Security Baseline Applied	WB-Win10-Hardened-v2.1	Confirms adherence to secure configuration standards.
Disposal Date	2027-04-01 (if applicable)	Date when the asset was formally disposed of.



<b>Disposal Method</b>	NIST Purge (Cryptographic Erase) + Physical Shred	Method used for data sanitization and physical disposal.
<b>Certificate of Destruction ID</b>	VENDOR-CERT-98765	Reference to auditable proof of secure data destruction.

- Value of Table:** This comprehensive IT Asset Register is the cornerstone of World Bank's ITAM program. For a financial institution, maintaining such a detailed and accurate inventory is not merely an operational best practice but a critical requirement for security and compliance. It enables effective risk management by identifying critical assets and their vulnerabilities, supports financial accountability through tracking of purchase and depreciation, ensures software license compliance, and provides an auditable trail for the entire lifecycle of an asset, including its secure disposal. This directly supports FFIEC requirements for asset inventory and ISO 27001 Annex A.8 controls , which are fundamental for protecting the Bank's information assets.