Asset Inventory

Document: Comprehensive IT Asset Inventory (hardware, software, data, key personnel, critical services)

- **Purpose:** To establish and maintain a detailed, centralized, and accurate record of all critical Information Technology (IT) assets owned, operated, or managed by or on behalf of the World Bank. This inventory serves as a foundational element for numerous cybersecurity and IT governance processes, including risk assessment, vulnerability management, configuration management, incident response, and compliance reporting. Without a clear understanding of what assets exist, where they are located, and their importance, effective protection is impossible.
- **Methodology and Maintenance:** The WDB recognizes that a comprehensive asset inventory for an organization of its scale and complexity is a significant and ongoing undertaking. Manual inventory methods alone are insufficient and prone to obsolescence. Therefore, the WDB's approach to asset inventory management incorporates:
    - **Automated Discovery Tools:** Deployment of network scanning and endpoint management tools to automatically discover and collect information about hardware and software assets connected to the WDB network (both on-premises and in cloud environments).
    - **Centralized Asset Management Database (AMDB):** All asset information is stored and managed in a central AMDB, which serves as the single source of truth. This database is designed to integrate with other IT service management (ITSM) and security tools (e.g., CMDB, vulnerability scanners).
    - **Consistent Asset Tagging:** All physical hardware assets are labeled with unique asset tags (e.g., barcodes or RFID tags) to facilitate physical inventory and tracking.
    - **Defined Ownership:** Each asset is assigned a technical owner (responsible for its operational maintenance) and, where applicable (especially for data assets and critical services), a business owner (Information Asset Owner, as per Section A.2).
    - **Lifecycle Management:** Processes are in place to record assets from procurement and deployment through to decommissioning and disposal. Status changes (e.g., In Use, In Repair, Spare, Retired) are tracked in the AMDB.
    - **Regular Audits:** Periodic physical and logical audits are conducted to verify the accuracy and completeness of the inventory and to identify any unauthorized or unrecorded assets.

  - **Integration with Other Processes:** The asset inventory is linked to other key processes, such as change management (updates to assets are reflected in the inventory), vulnerability management (vulnerabilities are mapped to specific assets), and incident response (identifying affected assets).

- **Scope of Assets:** The inventory covers a broad range of asset types:
  - **Hardware Assets:** Servers (physical and virtual), network devices (routers, switches, firewalls, load balancers), storage systems (SAN, NAS, tape libraries), workstations (desktops, laptops), mobile devices (smartphones, tablets issued by WDB), printers, and specialized financial hardware (e.g., secure terminals).
  - **Software Assets:** Operating systems, database management systems (DBMS), enterprise applications (e.g., core banking, ERP, CRM, HR systems – both COTS and custom-developed), desktop applications, security software (antivirus, EDR, DLP), development tools, and system utilities. Software licenses are also tracked.
  - **Data Assets:** Critical databases, significant data repositories, data warehouses, data lakes, and archives. For data assets, the inventory includes metadata such as the Information Asset Owner, data classification (cross-referenced with Section A.5), location, and retention period.
  - **Service Assets:** Critical IT services, both internal (e.g., email, directory services, file sharing) and external-facing (e.g., client web portal, API gateways). These are cross-referenced with the Critical IT Services Documentation (Section B.3).
  - **Cloud Assets:** Virtual machines, storage instances, databases, serverless functions, containers, and other resources deployed in Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) environments. This includes details of the cloud provider and region.
  - **Intellectual Property:** While primarily managed by IAOs, key IT-related intellectual property (e.g., source code for critical custom applications, proprietary algorithms embedded in systems) is referenced.

- **Inventory Fields:** The AMDB captures a comprehensive set of attributes for each asset. Key fields typically include :
  - Unique Asset ID
  - Asset Name/Hostname
  - Asset Category (Hardware, Software, Data, Service, Cloud)
  - Asset Type (e.g., Server, Router, Database, Application)
  - Description

- Manufacturer/Vendor
- Model/Version
- Serial Number/License Key
- Physical Location (Data Center, Building, Room, Rack) / Logical Location (URL, Cloud Region)
- Technical Owner (Team/Individual)
- Business Owner (IAO, if applicable)
- Purchase Date / Acquisition Date
- Warranty Expiry Date
- Deployment Date
- Last Audit Date
- Current Status (e.g., Production, Development, Test, Spare, Decommissioned, Disposed)
- Network Configuration (IP Address, MAC Address, VLAN)
- Operating System / Firmware Version (for hardware/software)
- Key Software/Applications Installed (for hardware)
- Dependencies (other assets it relies on, or that rely on it)
- Business Criticality (Critical, High, Medium, Low)
- Data Classification (for data assets or assets processing classified data)
- Maintenance Schedule/Contract Information
- Disposal Date and Method

IT Asset Inventory (Sample Extract)

The following table provides a highly abridged sample of entries that might be found in the WDB's IT Asset Inventory. A full inventory would contain thousands or tens of thousands of entries.

Asset ID	Asset Name	Category	Manufacturer	Model/Version	Location	Technical Owner (Team)	Status	Business Criticality	Data Classification (Hosts/Processes)
HW-SRV-001	Core Banking Application Server 1	Hardware	Dell EMC	PowerEdge R760	DC-LON-R01-U12 (London DC)	Core Systems Ops	Production	Critical	L3 - Restricted, L4 - Highly Restricted
HW-FWL-005	HQ Perimeter Firewall A	Hardware	Palo Alto Ntwk	PA-7050	HQ-NET-CORE-R05-U01 (HQ MDF)	Network Security	Production	Critical	N/A
SW-DBM-002	Client Loan Portfolio Database	Software	Oracle Corp	Database 19c Ent Ed	Runs on HW-SRV-CLS-010/011	Database Admin	Production	High	L3 - Restricted
SW-APP-015	Treasury Management System	Software	Finastra	Quantum Treasury v5.2	Runs on dedicated app servers	Treasury Systems Support	Production	Critical	L3 - Restricted
DATA-003	Global Economic Indicators DB	Data	WDB (Internal)	N/A	DW-PRD-DB01 (Data Warehouse)	Economic Research IAO	Production	High	L2 - Confidential (some L1 subsets)
SAAS-001	Human Resources Mgmt System	Cloud	Workday Inc.	Production Instance	Workday Cloud (EU Region)	HR Systems Admin	Production	High	L3 - Restricted
SVC-010	Enterprise Email Service	Service	Microsoft	Exchange Online (O365)	Microsoft Cloud	Collaboration Services	Production	High	Up to L3 - Restricted (in emails)