**ServiceNow CMDB Implementation Process**

**1. Introduction**

The Configuration Management Database (CMDB) in ServiceNow is a centralized repository that stores information about all the significant components of the IT environment. This document outlines the process for implementing a CMDB in ServiceNow.

InfoSec expects 100% inventory of all HAM and SAM assets across the environment.

Acceptance Criteria:

1. Search by employee/contractor and see all assets
2. Search by location
3. Search by floor
4. Search by dept
5. Search by AppOwner
6. Search by Support Engineer/Group
7. Avoid any manual update/entry to CI information

**2. Configuration Items (CIs)- Nebiyu**

Identify and categorize the Configuration Items (CIs) that need to be tracked in the CMDB. These include:

Asset tags should be

**Network Equipment**

* Switches
* Primary IP for each device
* Ports with IPs and device connected
* Routers
* Firewalls
* Network Load Balancers
* Appliances
* Wireless Access Points (WAPs)
* Uninterruptible Power Supplies (UPS)
* Wireless LAN Controllers (WLC)

Infoblox, Forscout, etc and standardized naming

* Location descriptions
* City
* Zip
* Classification normalization across source systems and how changes from one system drill down to other systems
* How do we identify HA devices with one logical name but two physical devices

**Windows Systems**

* Desktops
* Laptops
* Virtual Desktop Infrastructure (VDIs)
* Workstations
* Windows Tablets (Surface Pro)
* Servers (Physical, Virtual, Azure VMs, Windows 365, Azure Virtual Desktops)

**Linux Systems**

* VCenter Servers
* Horizon VDI
* Virtual Servers
* vROps
* System Health Information

**Mobile Devices**

* Mobile Phones (use ATT files for firm owned devices which includes
* Tablets
* Desk Phones
* IP Phones
* IPC Turrets (Trading Phones)

**Infrastructure**

* VxBlock (Hosts, Storage, Compute, RAM, Network)
* VxRail (Hosts, Storage, Compute, RAM)

**Security Appliances**

* Qualys
* RSA MFA

**Software Inventory**

* SCCM
* Archer

**3. Asset Management -** ( Tre Cole/Nate Jones for end user devices)

Track and manage the lifecycle of assets, including their ownership and relationships with other assets. This involves:

* Assigning assets to specific users or departments
* Tracking the status and location of assets
* Managing asset lifecycle events such as procurement, deployment, maintenance, and retirement

Sources:

1. Infoblox
2. Crowdstrike Falcon
3. Qualys
4. SCCM
5. MS Active Directory

These can be used to

Location of device, owner, who manages, IP, software inventory, etc;

**4. Service Catalog – Rob Zides and Nate Jones**

Document the services offered by the organization and how they relate to the CIs. This includes:

* Defining service offerings and their components
* Mapping services to the underlying CIs
* Establishing service level agreements (SLAs) and performance metrics

**5. Incident Management – Nebiyu**

Implement processes and workflows for managing incidents related to the CIs. This involves:

* Logging and categorizing incidents
* Assigning incidents to appropriate support teams and managing of queues by each platform owner and team (Service operations dashboard)
* Escalation process for each incident related to each application and/or platform
* Attach SLAs to each incident based on impact and category
* Tracking incident resolution and closure

**6. Change Management- Nebiyu/Joe/Robert**

Establish procedures for handling changes to the CIs, including:

* Requesting and approving changes
* Notifying stakeholders of planned changes
* Implementing and validating changes
* Documenting change history and impact

**7. Automated Test Platform – SNOW Dev Team**

Integrate automated testing processes and tools to ensure the accuracy and reliability of the CMDB. This includes:

* Setting up automated tests for CI data validation
* Monitoring test results and addressing issues
* Continuously improving test coverage and effectiveness

**8. Architecting Solutions – Gap**

Design and implement solutions on the ServiceNow platform to support the CMDB. This involves:

* Customizing ServiceNow tables and forms to capture CI data
* Developing workflows and automation scripts
* Integrating with other IT systems and data sources

**9. Support and Escalation- TechOps**

Define support groups and escalation points for managing CIs. This includes:

* Mapping hardware and software to the appropriate support groups
* Identifying managers and escalation points for each support group
* Establishing procedures for escalating issues and tracking resolution

**10. ServiceNow Destination Information – TechOps**

Determine the ServiceNow tables to use for storing CI data. This includes:

* Computers
* Network Equipment (IP Routers, IP Switches)
* Existing processes (e.g., SQL Server stored procedures for D42/Qualys process prior to going to ServiceNow)

**11. ServiceNow Knowledge**

* Centralized location for IT support documentation by application owners
* Business user documeantion created and maintained by application owners

**12. ServiceNow API/Integrations**

* Automation and orchestration of SRs and tasks for user access and onboarding/offboarding starting from Workday
* Helpdesk integrations
* Ring Central
* OpsGenie
* Nexthink
* Axonius
* Mobility (SNOW mobile app)
* Tableau
* Email/Outlook - ITsupport>incident>updates to users